Penetracja systemu i sieci komputerowych

WIELE CZYNNIKÓW ZWIĄŻANYCH Z PNETRACJĄ SYSTEMU

Chociaż penetracja systemów i sieci komputerowych może wydawać się wyzwaniem technicznym, większość specjalistów ds. bezpieczeństwa informacji ma świadomość, że bezpieczeństwo systemów ma zarówno aspekty techniczne, jak i nietechniczne. Oba aspekty wchodzą w grę, gdy ludzie próbują przeniknąć do systemów. Oba aspekty zostały omówione w tej części, która nie jest instrukcją dotyczącą sposobu penetracji systemów, ale raczej przeglądem metod i środków, za pomocą których dokonuje się penetracji systemów.

BEZPIECZEŃSTWO SYSTEMU : WIĘCEJ NIŻ PPROBLEM TECHNICZNY

Podstawowym nietechnicznym czynnikiem bezpieczeństwa systemu i odporności na penetrację systemu jest zachowanie człowieka, które może pokonać niemal każdy techniczny środek bezpieczeństwa. Bardziej niż cokolwiek innego, bezpieczeństwo zależy od ludzi, aby zrozumieć i przeprowadzić procedury bezpieczeństwa. W związku z tym bezpieczeństwo systemu informatycznego (IS) musi być integralną częścią kultury każdej organizacji stosującej system informacyjny. Bez zabezpieczeń systemy i sieci nie będą w stanie oprzeć się próbom penetracji. Często bezpieczeństwo reprezentowane jest jako struktura koncentrycznych kół. Ochrona centralnego, zabezpieczonego elementu zależy wówczas od barier nałożonych przez każdy kolejny pierścień. Bariery te mogą być fizyczne lub symboliczne, ale celem bezpieczeństwa SI jest ochrona integralności, poufności i dostępności informacji przetwarzanych przez system. Cel ten osiąga się za pomocą identyfikacji, uwierzytelniania i autoryzacji. Identyfikacja jest warunkiem wstępnym, a każdy użytkownik musi podać identyfikator (ID), który znajduje się na listach autoryzacji systemu, do którego można uzyskać dostęp. Uwierzytelnianie polega na udowodnieniu, że użytkownik jest naprawdę osobą, do której przypisano identyfikator. Autoryzacja polega na zdefiniowaniu, co konkretny identyfikator użytkownika, uruchamiając określone programy, może legalnie zrobić w systemie. Obwód bezpieczeństwa można przeniknąć, naruszając którąkolwiek z tych funkcji. Trend w kierunku komputerów rozproszonych i mobilnych, często wykorzystujących możliwości globalnej sieci w Internecie, sprawia, że trudno jest wiedzieć, gdzie jest narysować koncentryczne kręgi ochrony. Rzeczywiście, bariery penetracji należy rozszerzyć wzdłuż linii komunikacyjnych, obejmujących punkty końcowe sieci, które mogą być rozproszone geograficznie.

KULTURA ORGANIZACYJNA

Ogólne podejście organizacji do bezpieczeństwa jest kluczem do skutecznej obrony przed atakiem. Bezpieczeństwo trudno sprzedać, zwłaszcza organizacji, która nigdy nie doświadczyła znaczącego problemu. (Jak na ironię, im lepsza ochrona, tym mniej dowodów na ich użyteczność.) Podstawową zasadą bezpieczeństwa jest to, że praktykujący muszą zachowywać się tak, jakby byli paranoikami, nieustannie strzegąc przed atakami z dowolnego kierunku. Wiele organizacji postrzega środki bezpieczeństwa jako atak na uczciwość pracowników. Na przykład noszenie odznak jest czasem postrzegane jako odczłowieczające i obraźliwe. Takie podejście prowadzi do absurdów, takich jak noszenie odznak tylko przez odwiedzających. Jeśli tylko goście noszą odznaki, zdjęcie odznaki automatycznie zmniejsza prawdopodobieństwo, że nieuczciwy intruz zostanie zakwestionowany. Niektórzy indywidualni pracownicy uważają również środki ostrożności za obraźliwe. Na przykład zablokowanie terminala lub stacji roboczej podczas opuszczania go na kilka minut może być postrzegane jako dowód nieufności wobec innych pracowników. Odmowa zezwolenia na korzystanie - czyli umożliwienie kilku kolegom wejścia na ograniczony obszar na jednej karcie dostępu - może być postrzegana jako nieuprzejmie niegrzeczne. Tam, gdzie uczy się pracowników otwartości a kolegialne, zabezpieczanie wymiennych nośników komputerowych i dokumentów w nocy może wydawać się

obraźliwe. Konflikty te występują, ponieważ lata socjalizacji, zaczynając od niemowlęctwa, są diametralnie przeciwne zasadom bezpieczeństwa informacji. Uprzejmość w kontekście społecznym jest katastrofą w bezpiecznym obszarze; na przykład, piggybacking do sali komputerowej pogarsza dokładność ścieżek audytu prowadzonych przez komputery kontroli dostępu. Pożyczanie samochodu jest miłe i hojne, ale pożyczanie komuś identyfikatora użytkownika i osobistego hasła jest rażącym naruszeniem odpowiedzialności. Realizacja skutecznych polityk i procedur bezpieczeństwa musi rozwiązać te konflikty między normalnymi standardami grzeczności a standardami wymaganymi w bezpiecznym środowisku. Organizacje muszą wspierać otwartą dyskusję na temat stosowności procedur bezpieczeństwa, aby pracownicy mogli dobrowolnie tworzyć kulturę korporacyjną sprzyjającą ochronie informacji korporacyjnych. Poza tym organizacje muszą być świadome postawy bezpieczeństwa i postaw osób, z którymi się łączą. W dzisiejszych czasach system jednej organizacji może być obsługiwany, a nawet własnością innej,. I ludzie z wielu różnych organizacji mogą korzystać z tej samej sieci. Kultura bezpieczeństwa musi przenikać wszystkie organizacje, które mają dostęp do systemu, w przeciwnym razie będą istnieć punkty słabości, zwiększając w ten sposób prawdopodobieństwo, że próby penetracji systemu zakończą się sukcesem

NIETECHNICZNE TECHNIKI PENETRACJI.

Chociaż penetracja systemów informatycznych jest często przedstawiane jako praca biegłego technicznie, wiele udanych penetracji opierało się na czynnikach ludzkich, takich jak łatwowierność i żywotność. Oba są wykorzystywane przez potencjalnych penetratorów systemu.

WPROWADZENIE W BŁĄD (INŻYNIERIA SPOŁECZNA)

Inżynieria społeczna opiera się na fałszu. Kłamstwa, łapówki i uwodzenie mogą oszukać uczciwych lub nieznacznie nieuczciwych pracowników w celu ułatwienia penetracji. Osoba atakująca może nakłonić pracownika do ujawnienia kodów logowania i uwierzytelnienia, a nawet do fizycznego dostępu do bezpiecznej witryny. Penetrację systemu można następnie osiągnąć na wiele sposobów, od przejścia do niezabezpieczonej stacji roboczej, po zainstalowanie kodu trojana lub urządzenia do wykrywania pakietów sieciowych.

KŁAMSTWO

Mówienie kłamstw jest techniką często stosowaną przez osoby zamierzające uzyskać nieautoryzowany dostęp do systemu. Cenne informacje o systemie i jego obronie można uzyskać, kłamiąc. Wiele kłamstw działa, grając na naturalnej ludzkiej skłonności do interpretowania świata przez nasz wewnętrzny model tego, co najprawdopodobniej. Psychologowie społeczni nazywają ten model schematem. Dobrze ubrani biznesmeni, którzy energicznie chodzą i asertywnie mówią. W rozmowie telefonicznej osoba, która wydaje się zirytowana, niecierpliwa i niegrzeczna, gdy żąda nowego hasła, jest prawdopodobnie zirytowanym, niecierpliwym i niegrzecznym pracownikiem, który zapomniał hasła. Niestety, wielu przestępców wie, czasami instynktownie, jak wykorzystać te interpretacje, aby pomóc im dostać się do zabezpieczonych systemów. Inną techniką, często stosowaną w połączeniu z kłamstwem, jest uniknięcie zauważenia i uniknięcie podejrzeń poprzez zwykłe wtopienie się w to. Sposób, w jaki postrzegamy lub nie dostrzegamy szczegółów, określany jest przez psychologów społecznych jako problem podstawowy. Normalna staje się tłem, a obiekty naszej uwagi stają się postaciami wyróżniającymi się z ziemi. Schemat wpływa na to, co jest zauważane; jedynie odchylenia od oczekiwań powodują dyskryminację opartą na liczbach. Hakerzy kryminalni wykorzystują ten efekt, znikając w tle, jednocześnie penetrując obwody bezpieczeństwa.

PODSZYWANIE SIĘ POD AUTORYZOWANY PESONEL

Kryminalni hakerzy i pozbawieni skrupułów pracownicy dzwonią do pracowników ochrony, operatorów, programistów i administratorów, aby żądać identyfikatorów użytkowników, uprawnień, a nawet haseł. (Jest to jeden z powodów, dla których telefon jest słabym medium do nadawania uprawnień bezpieczeństwa; jeśli pracownicy zostali przeszkoleni w zakresie odrzucania wniosków składanych przez telefon, wiele prób przeniknięcia do systemów może zostać udaremnionych). W miejscach, gdzie pracownicy noszą identyfikatory, intruzi mają trudność z przeniknięciem do bezpieczeństwa fizycznego przez udawanie pracowników. Jednak bezpieczeństwo fizyczne w tych przypadkach zależy od współpracy wszystkich upoważnionych pracowników w celu rzucenia wyzwania każdemu, kto nie nosi plakietki. Ta polityka jest niezwykle ważna w punktach wejścia. Aby fizycznie przeniknąć do takich witryn, przestępcy muszą ukraść lub wykuć odznaki lub współpracować z konfederatami w celu uzyskania prawdziwych, ale nieautoryzowanych odznak. Witryny, w których bezpieczeństwo fizyczne obejmuje fizyczne tokeny, takie jak karty do elektronicznej kontroli dostępu, są trudniejsze do penetracji przez przestępców. Muszą uzyskać prawdziwy token, być może przez kradzież lub zmowę z pracownikiem. Bezpieczeństwo obwodowe zależy od aktualizacji kodów dostępu, aby karty należące do byłych pracowników były nieaktywne. Pracownicy ochrony muszą natychmiast dezaktywować wszystkie zgubione karty. Ponadto istotne jest, aby pracownicy nie zezwalali na piggybacking, czyli czynność pozwalającą innej osobie, być może nieupoważnionej, na wjazd do strefy zamkniętej wraz z osobą upoważnioną. Zbyt często pracownik, w grzeczności, pozwala innym wejść do normalnie zamkniętych drzwi, gdy wychodzi. Wewnątrz budynku przestępcy mogą ukraść cenne informacje, które umożliwią późniejszą penetrację systemów komputerowych ze zdalnych lokalizacji. Często osiąga się to poprzez podszywanie się pod personel zewnętrzny. Nawet jeśli pracownicy są gotowi rzucić wyzwanie odwiedzającym w garniturach biznesowych, może nie przychodzić im na myśl, aby ingerować w ludzi, którzy wyglądają, jakby byli pracownikami autoryzowanej firmy wsparcia. Na przykład złodziejom często udawało się wejść do strefy chronionej, ubierając się jak technicy komputerowi lub sprzątacze biur. Niewielu pracowników pomyśli o sprawdzeniu wiarygodności znużonego technika w brudnym kombinezonie, autentycznie wyglądającej firmowej plakietce, kolorowym dowodzie osobistym i pasku narzędzi. Kiedy odpowiedni pracownik twierdzi, że został wezwany do przeprowadzenia diagnostyki na stacji roboczej, wielu nietechnicznych pracowników zgodzi się natychmiast, korzystając z okazji, aby napić się kawy lub porozmawiać z kolegami. Kilka minut później złodziej mógł skopiować poufne pliki lub zainstalować urządzenie podsłuchujące (np. rejestrator naciśnięć klawiszy lub sniffer pakietów sieciowych). W jednym przypadku znanym jednemu z autorów (MK) przestępcy otrzymał obszar roboczy i połączenie sieciowe w dużym banku i pozwolono mu na pracę przez kilka miesięcy w sposób niezamierzony i niekwestionowany przy „tajnym projekcie". ochroniarz zdał sobie sprawę, że nikt w biurze nie wiedział, kim jest ta osoba, że rzuciła wyzwanie intruzowi i złamała oszustwo.

ZASTRASZENIE

Techniką związaną z podszywaniem się pod uprawnionego lub osoby trzecie jest zastraszanie. Ktoś podający się za osobę na stanowisku władzy wykazuje irytację lub złość z powodu opóźnień w przyznaniu nieautoryzowanego odstępstwa od zasad, takich jak przekazanie hasła przez telefon osobie o nieuwierzytelnionej tożsamości. Atakujący pośrednio lub bezpośrednio grożą niepokojącymi konsekwencjami (np. opóźnieniami krytycznych napraw, strat finansowych, działań dyscyplinarnych), chyba że otrzymają ograniczone informacje lub dostęp do zabezpieczonego sprzętu lub urządzeń.

OBALENIE

Ludzie stale dokonują moralnych wyborów. Zawsze istnieje świadome lub nieświadome równoważenie alternatyw. Hakerzy kryminalni starają się osiągnąć swoje cele, zmieniając zasady, tak aby nieuczciwość stała się bardziej akceptowana dla ofiary niż uczciwość.

PRZEKUPSTWO

Wiele informacji przemysłowych i handlowych ma wartość czarnego rynku. To samo dotyczy danych osobowych, które można wykorzystać do popełnienia oszustwa i kradzieży tożsamości. Cena planów inżynieryjnych lub bazy danych klientów konkurenta może stanowić roczną pensję dla operatora komputerowego odpowiedzialnego za tworzenie kopii zapasowych. Niewielkie prawdopodobieństwo, że ktokolwiek zauważy, że zbuntowany operator kopiuje kopię zapasową o 3:00 rano lub sekretarka wynosząca dodatkową płytę kompaktową z biura. Wiele organizacji nie zainstalowało oprogramowania, aby uniemożliwić menedżerowi wysyłanie poczty elektronicznej z poufnymi plikami do przyszłego pracodawcy. Fakt, że szpiegostwo przemysłowe, ze sponsorem państwowym lub bez niego, jest dobrze prosperującym biznesem, jest faktem, który jest obecnie powszechnie - a czasem dość otwarcie - uznawany. Budowanie środowiska korporacyjnego, w którym pracownicy słusznie czują się częścią społeczności, jest ostoją przeciw szpiegostwu. Gdy szacunek i poczucie zamiany na wzajemne korzyści będą miały wpływ na kulturę korporacyjną, pracownicy odrzucą szpiegów, a nawet aresztują ich, ale niezadowolony pracownik, którego potrzeby nie są zaspokojone, jest potencjalnym wrogiem

UWODZENIE

Czasami hakerzy i szpiedzy kryminalni uzyskali poufne informacje, w tym kody dostępu, oszukując pracowników, aby uwierzyli, że są kochani. To kłamstwo działa wystarczająco dobrze, aby umożliwić dostęp do rzeczy osobistych, czasami po tym, jak fałszywa pasja lub narkotyki doprowadziły ofiarę do niewrażliwości. Wiadomo, że prostytutki uwodzą mężczyzn z organizacji, które one i ich zleceniodawcy próbują złamać. Przeszukując portfele klientów często można odkryć charakterystyczne kupony z identyfikatorami użytkowników i hasłami. Nikt nie może zapobiec wszelkim takim nadużyciom. Ludzie zafascynowani doświadczonymi manipulatorami rzadko podejrzewają, że są wykorzystywani jako kliny przez obwód bezpieczeństwa. Wraz z ogólnym wzrostem świadomości bezpieczeństwa pracownicy z wrażliwymi kodami muszą zdawać sobie sprawę z tych technik, aby byli mniej podatni na zagrożenia. Być może wtedy automatycznie odrzucą prośbę o poufne informacje lub kody dostępu.

WYMUSZENIE

Przestępcy mogą zagrozić krzywdą, jeśli ich żądania nie zostaną spełnione. Zagrażaj czyjejś rodzinie lub trzymaj broń przy głowie, a niewielu będzie lub powinno się oprzeć żądaniu wejścia do zabezpieczonego obiektu lub sekwencji logowania do sieci. Niektóre fizyczne systemy kontroli dostępu zawierają sygnał przymusu, którego można użyć do wyzwolenia cichego alarmu na stacjach monitorowania. Sygnał przymusu wymaga z góry określonej, celowej akcji ze strony osoby zmuszanej do przyjęcia nieupoważnionego personelu. To działanie może polegać na dodaniu dodatkowego numeru do normalnego kodu dostępu, dwukrotnym naciśnięciu znaku funta (#) po wprowadzeniu kodu lub wpisaniu 4357 (H-E-L-P) na klawiaturze. Sygnał przymusu potajemnie informuje o bezpieczeństwie, że pracownik jest zmuszany do robienia czegoś niechętnie. Bezpieczeństwo może wówczas podjąć odpowiednie działania.

SZANTAŻ

Szantaż to wymuszenie oparte na groźbie ujawnienia tajemnic. Pracownik może zostać uwięziony w ujawnieniu poufnych danych, na przykład przy użyciu właśnie opisanych technik. Klasyczny szantaż obejmuje uwodzenie, a następnie zdjęcia w flagrante delicto, które przestępcy grożą ujawnieniem. Czasami osobę można wrobić w sfabrykowane dowody; wiarygodny, ale sfałszowany obraz okolicy może zrujnować karierę równie łatwo jak prawda. Zdrowy szacunek dla osób i więzi społeczne między pracownikami, przełożonymi i zarządem mogą utrudnić szantażystom odniesienie sukcesu. Jeśli

pracownicy, którzy padli ofiarą szantażu, uważają, że mogą poinformować zarząd bez ponoszenia niewłaściwie negatywnych konsekwencji, zagrożenie można w pewnym stopniu złagodzić. Być może ostatnią, najlepszą obroną przed szantażem jest uczciwość. Wyjątkowo uczciwa osoba odrzuci okazje, które prowadzą do wiktymizacji poprzez szantaż, i będzie się śmiać z fabrykacji, ufając, że znajomi i koledzy rozpoznają kłamstwa, gdy je usłyszą.

WEWNĄTRZ

Wiele największych i najodważniejszych napadów na świecie po zbadaniu, okazało się być wykonane w miejscach pracy. To samo dotyczy penetracji systemu. Chociaż wiele z właśnie opisanych technik może zostać wykorzystanych do uzyskania pomocy z wewnątrz, niektóre z nich są możliwe przez osoby wewnątrz, które z jakiegokolwiek powodu decydują się na pomoc hakerom. Na przykład nieuczciwy pracownik może aktywnie starać się sprzedać dostęp dla osobistych korzyści. Organizacje powinny starać się zwracać uwagę na tę ewentualność, ale bardzo mało jest obrony przed całkowicie nieuczciwymi pracownikami, gdy jedynym jawnym czynem koniecznym do otwarcia bram od wewnątrz jest przekazanie poświadczeń systemowych osobie z zewnątrz

ZASIĘG DOCELOWY DLA LUDZI

Organizacje nie powinny lekceważyć zakresu celów, do których mogą być skierowane opisane techniki. Mimo że w poprzednich akapitach użyto terminów pracownicy, upoważniony personel i personel zewnętrzny, docelowy zakres obejmuje wszystkich dostawców, dostawców i wykonawców, a także wszystkie poziomy pracowników - od dostawców oprogramowania i sprzętu, przez programistów kontraktowych , do dostawców napojów bezalkoholowych i personelu sprzątającego. Może nawet obejmować klientów i klientów, z których niektórzy posiadają szczegółową wiedzę na temat działalności organizacji. Pracownicy na każdym poziomie prawdopodobnie znają się na komputerach, choć mają różny poziom umiejętności. Na przykład jest całkiem możliwe, że ktoś pracujący dzisiaj jako dozorca wie, jak umiejętnie obsługiwać komputer, a nawet umie surfować po witrynach hakerskich w Internecie i pobierać narzędzia penetracyjne. Rzeczywiście woźny mógł zdobyć pracę specjalnie z zamiarem angażowania się w szpiegostwo przemysłowe, kradzież danych lub sabotaż. Krótko mówiąc, każdy, kto wejdzie w kontakt z organizacją, może przekazać osobie atakującej informacje przydatne w przygotowaniu i przeprowadzeniu ataku. Ludzkie cele ataku socjotechnicznego nie mogą, indywidualnie, posiadać ani ujawniać krytycznych informacji, ale każdy może dostarczyć wskazówek - elementów układanki - których agregacja może doprowadzić do udanej penetracji i kompromisu cennych danych i zasobów. Wykorzystanie tego procesu jest znakiem rozpoznawczym niektórych z najbardziej skutecznych hakerów kryminalnych. Określenie przyrostowe pozyskiwanie informacji wymyślono dla tego wykorzystania mniej wartościowych danych w celu uzyskania bardziej wartościowych danych

WYKORZYSTYWANIE INFORMACJI PRZYROSTOWYCH

Gromadząc i zręcznie wykorzystując małe i pozornie nieistotne informacje, można uzyskać dostęp do znacznie cenniejszych informacji. Ta technika przyrostowego wykorzystywania informacji jest ulubionym narzędziem hakerów, zarówno kryminalnych, jak i innych. Jedną ważną zaletą narzędzia, które jest szczególnie doceniane przez hakerów kryminalnych, jest niski profil, jaki przedstawia większości form wykrywania. Gromadząc pozornie nieszkodliwe informacje przez pewien czas i dokonując inteligentnych wniosków na ich podstawie, można przeniknąć do systemów na najwyższym poziomie. Doskonałym przykładem tego podejścia są wyczyny Kevina Mitnicka, który przez prawie pięć lat siedział za kratkami za włamanie do komputerów, kradzież danych i nadużywanie systemów komunikacji elektronicznej. Nielegalne czyny popełniane przez Mitnicka obejmują penetrację w 1981 roku Systemu komputerowego dla operacji na komputerach mainframe (COSMOS), budynku Pacific

Bell w centrum Los Angeles. COSMOS była scentralizowaną bazą danych wykorzystywaną przez wiele amerykańskich firm telefonicznych do kontrolowania podstawowych funkcji prowadzenia rejestrów. Mitnick i inni minęli ochroniarza i znaleźli pomieszczenie komputerowe COSMOS. Ukradli listy haseł komputerowych, instrukcje obsługi systemu COSMOS oraz kombinacje zamków do drzwi w dziewięciu centralnych biurach Pacific Bell. Później Mitnick wykorzystał znajomość systemów telefonicznych i operacji firmy telefonicznej do penetracji systemów w Digital Equipment Corp. (DEC). Od czasu wydania w styczniu 2000 r. Mitnick mówił o bezpieczeństwie informacji przed Kongresem i w innych miejscach publicznych. Opisał inżynierię społeczną jako tak potężne narzędzie, że „rzadko musiał uciekać się do technicznego ataku". Jeśli chodzi o technikę, stwierdził: „Dużo improwizowałem. . . Próbowałbym nauczyć się ich wewnętrznego żargonu i ciekawostek, które zna tylko pracownik. "Innymi słowy, budując wiedzę o celu, korzystając z wielu informacji, które nie są ani chronione, ani zastrzeżone, można uzyskać dostęp do tego, co jest zarówno zastrzeżone, jak i chronione. Moc przyrostowej dźwigni informacji jest odpowiednikiem przekształcenia stopy w drzwi w zaproszenie do wejścia do środka. Ochrona przed przyrostowym wykorzystywaniem informacji i wszystkimi innymi aspektami inżynierii społecznej zaczyna się od świadomości pracowników. Pracownicy, którzy zachowują zdrowy sceptycyzm wobec wszelkich wniosków o udzielenie informacji, zapewniają silną linię obrony. Kolejnym potężnym mechanizmem obronnym, na który zwrócił uwagę Mitnick, jest wykorzystanie wiadomości telefonicznych, takich jak: „Ta wiadomość może być monitorowana lub nagrywana w celach szkoleniowych i zapewniania jakości". Osoba atakująca, która słyszy taką wiadomość, może dwa razy pomyśleć o podejmowaniu prób używać połączeń głosowych do informacji inżyniera społecznościowego od celu.

TECHNICZNE TECHNIKI PENETRACJI

Techniczne ataki penetracyjne mogą opierać się na danych uzyskanych z inżynierii społecznej lub mogą być przeprowadzane wyłącznie na podstawie technicznej. Stosowane techniki obejmują podsłuch, słuchając rozmów lub zatrzymując dane podczas transmisji, oraz naruszenia kontroli dostępu (np. wypróbowanie wszystkich możliwych haseł dla identyfikatora użytkownika lub odgadnięcie haseł). Niedociągnięcia w projektowaniu i wdrażaniu systemów informatycznych, takie jak błędy programowe i brak sprawdzania poprawności danych wejściowych, mogą być również wykorzystywane w atakach technicznych. Niestety tego rodzaju słabości obfitują w sferę Internetu, nawet gdy coraz więcej organizacji zwiększa łączność z Internetem, tworząc w ten sposób coraz więcej potencjalnych punktów penetracji.

WYCIEK DANYCH : PODSTAWOWY PROBLEM

Niestety, dla specjalistów ds. bezpieczeństwa informacji (INFOSEC), nawet teoretycznie niemożliwe jest zapobieganie nieautoryzowanemu przepływowi informacji z zabezpieczonego regionu do niezabezpieczonego regionu. Niewidoczny transfer danych bez autoryzacji znany jest jako wyciek danych. Same środki techniczne nie mogą powstrzymać wycieku danych. Rozważ ściśle zabezpieczony system operacyjny lub monitor bezpieczeństwa, który zapobiega kopiowaniu poufnych danych do niezabezpieczonych plików. Stacje robocze są bezdyskowe, nie ma drukarek, pracownicy nie zabierają dysków do zabezpieczonego obiektu lub z nich, a także istnieją surowe ograniczenia dotyczące usuwania wydruków z budynku. Mechanizmy te powinny wystarczyć, aby zapobiec wyciekom danych.

Nie całkiem.

Każdy, kto ma zamiłowanie do mnemoniki lub ma pamięć fotograficzną, może po prostu zapamiętać informacje i zapisać je po wyjściu z obiektu. Niezwykle trudno jest też uniemożliwić pracownikom pisanie notatek na papierze i ukrywanie ich w ubraniach lub dobytku osobistym, gdy wychodzą z pracy. O ile pracownicy nie zostaną przeszukani, żaden strażnik nie będzie w stanie powstrzymać ludzi ze

ściagwkami pełnymi poufnych danych przed wyjściem z budynku. Rzeczywiście, w ten sposób Wasilij Mitrokhin, główny archiwista Pierwszej Naczelnej Dyrekcji KGB, dopuścił się największego naruszenia bezpieczeństwa KGB w historii, przemycając tysiące swoich odręcznych kopii tajnych dokumentów z siedziby głównej KGB w Moskwie w swoich butach, skarpetach i innej odzieży. Innym sposobem wycieku danych jest steganografia, ukrywająca cenne informacje na widoku wśród dużej ilości nietypowych informacji. Na przykład skorumpowany pracownik zdecydowany wysłać konfederacyjną informację o wzorze chemicznym może zakodować tekst jako ekwiwalenty liczbowe i wydrukować te wartości jako, powiedzmy, czwartą i piątą cyfrę zestawu cyfr inżynierskich. Nikt prawdopodobnie nie zauważy, że liczby te zawierały coś specjalnego. Bardziej skłonni cyfrowo mogą używać oprogramowania steganograficznego, dostępnego bezpłatnie w Internecie, do ukrywania danych w plikach obrazów. Nie można całkowicie zapobiec nieautoryzowanemu przekazywaniu informacji, ponieważ informacje mogą być przekazywane za pomocą wszystkiego, co może się zmieniać. Teoretycznie można przenieść dane do wspólnika, zmieniając położenie zasłony okna (powoli, ale możliwe). Lub można przesyłać jedynki i zera według kierunku drgań szpuli; lub można wysłać zakodowane informacje przez wybór muzyki. Nawet jeśli budynek byłby całkowicie zamknięty, nadal przenikałby ciepło na zewnątrz lub przenosił ciepło do wewnątrz - i to wystarczało do przenoszenia informacji. W praktyce menedżerowie systemów mogą najlepiej rozwiązać problem wycieku danych dzięki połączeniu ochrony technicznej i skutecznych strategii zarządzania. Ważne jest również, aby zdawać sobie sprawę, że znaczna ilość wycieków danych występuje w wyniku nieszkodliwych zamiarów komunikacji od pracowników. Pracownicy często dyskutują o małych aspektach swojej pracy i informacji o pracy, nie zdając sobie sprawy z konsekwencji i zdolności innych osób do zestawiania tych informacji w znacznie większych ilościach. Stało się to szczególnie rozpowszechnione wraz z pojawieniem się mediów społecznościowych. Mogą być znaczące ilości informacji o organizacji i jej wewnętrznych działaniach pochodzące ze stron pracowników mediów społecznościowych. W związku z tym media społecznościowe stały się bogatym źródłem danych dla atakujących, którzy chcą atakować organizację. Takie podejście jest szczególnie powszechne wśród atakujących organizację za pośrednictwem jej pracowników przy użyciu technik takich jak phishing spear. Zapobieganie utracie danych (DLP) to obecnie ustalony zestaw technik z licznymi narzędziami do egzekwowania ograniczeń dotyczących nieautoryzowanego przesyłania danych do urządzeń pamięci masowej i witryn zewnętrznych. Niemniej jednak czujność wobec ludzkich zachowań i skuteczna konfiguracja oraz analiza zapisów dziennika w czasie rzeczywistym lub przynajmniej częsta pozostają podstawowymi elementami skutecznego DLP.

PRZECHWYTYWANIE KOMUNIKACJI

Hakerzy kryminalni oraz nieuczciwi lub niezadowoleni pracownicy mogą uzyskiwać kody dostępu i inne informacje przydatne w ich wysiłkach związanych z penetracją systemu poprzez monitorowanie komunikacji. Mogą to być między dwiema stacjami roboczymi w sieci lokalnej lub rozległej, między zdalnym terminalem a hostem, takim jak komputer mainframe, lub między klientem a serwerem w Internecie. Atakujący mogą wykorzystać różne luki w technologiach komunikacyjnych. Przejście na komunikację internetową opartą na protokole transmisji / protokole internetowym (TCP / IP) w ciągu ostatniej dekady spowodowało, że o wiele więcej strumieni komunikacyjnych trafiło do docelowego zakresu potencjalnych penetratorów

PODSŁUCH

Podsłuchiwanie polega na przechwytywaniu strumienia danych w kanale komunikacyjnym (nawet jeśli ten kanał nie jest przewodowy; np. Kabel światłowodowy może być również stukany, podobnie jak komunikacja bezprzewodowa, chociaż te ostatnie czasami są raczej wąchane niż podsłuchiwane).

KOMUNIKACJA ASYNCHRONICZNA

Połączenia danych typu punkt-punkt (np. za pomocą modemów telefonicznych lub urządzeń szeregowych) prawie zniknęły, ale ich relacja jest stosunkowo łatwa. Fizyczne połączenie w dowolnym punkcie skrętki lub kabli wielożyłowych pozwala podsłuchiwać rozmowy; jeśli linia jest używana do przesyłania danych, łatwo można podłączyć monitor, aby wyświetlać i rejestrować wszystkie informacje przesyłane między węzłem a jego hostem. Linie asynchroniczne w dużych instalacjach często przechodzą przez panele krosowe, w których zajęty personel pomocniczy może nie zauważyć stuknięć, ponieważ zarządzają setkami legalnych połączeń. Taka komunikacja zwykle wykorzystuje linie telefoniczne na odległości przekraczające kilkaset metrów (lub około 1000 stóp). Wiretaperzy muszą używać modemów skonfigurowanych dla poprawnych parametrów komunikacji, w tym prędkości, parzystości, liczby bitów danych i liczby bitów stopu, ale parametry te można łatwo ustalić metodą prób i błędów. Środki zaradcze obejmują:

* Fizyczne ekranowanie kabli i paneli krosowych

* Multipleksowanie strumieni danych na tych samych przewodach

* Szyfrowanie danych przepływających między węzłami i hostami

KOMUNIKACJA SYNCHRONICZNA

Ponieważ modemy synchroniczne są bardziej złożone niż modele asynchroniczne i ponieważ ich przepustowości (maksymalne prędkości transmisji) są wyższe, są mniej podatne na atak, ale nie są wolne od ryzyka.

LINIE TELEFONICZNE DIAL-UP

Wykorzystywane zarówno do transmisji danych, jak i głosu, linie telefoniczne dostarczane przez lokalnych operatorów telefonicznych i operatorów długodystansowych są narażone na podsłuch. Organy ścigania i pracownicy firmy telefonicznej mogą instalować krany przy centralnym przełączaniu. Przestępcy mogą podłączać linie telefoniczne w budynku za pomocą paneli krosowniczych, kolektorów kablowych biegnących w sufitach podwieszanych, pod podniesionymi podłogami lub nawet w płytach kartonowo-gipsowych. Mogą także stukać w puszki połączeniowe, w których linie łączą się z kablami zewnętrznymi operatora telefonicznego. Te same środki zaradcze dotyczą linii telefonicznych jak asynchronicznych lub synchronicznych kabli do transmisji danych

LINIE DZIERŻAWIONE

Linie dzierżawione korzystają z tej samej technologii co linie telefoniczne (przełączane), z tym wyjątkiem, że operator telefoniczny zapewnia stałą sekwencję połączeń zamiast losowego przełączania z jednej stacji centralnej na drugą. W linii dzierżawionej nie ma nic bardziej bezpiecznego niż linia przełączana; wręcz przeciwnie, łatwiej jest wykorzystać linię dzierżawioną w centrali, ponieważ jej ścieżka jest stała. Jednak dzierżawione linie zwykle wykonują transmisje o dużej objętości. Im większa objętość zmultipleksowanych danych, tym trudniejsze jest dla amatorów potwierdzenia rozplątanie strumieni danych i ich zrozumienie. Na najwyższym poziomie przepustowości dzierżawionej linii (np. Operatorzy, tacy jak T1, T2 itp.), Koszt sprzętu multipleksującego sprawia, że przechwytywanie jest niezwykle kosztowne dla wszystkich osób poza podsłuchami profesjonalnymi lub rządowymi. Szyfrowanie danych zapewnia najlepszą ochronę przed podsłuchiwaniem łączy dzierżawionych.

TRANSMISJA NA DUŻE ODLEGŁOŚCI

Linie telefoniczne i dzierżawione obsługują transmisje zarówno na krótkich dystansach, jak i na duże odległości. Te ostatnie wprowadzają dodatkowe punkty podatności. Wieże przekaźników mikrofalowych przenoszą większość dalekosiężnej komunikacji głosowej i danych na kontynencie. Wieże są oddalone od siebie o około 40 kilometrów ; sygnały rozchodzą się zauważalnie na takich odległościach. Odbiorniki radiowe na poziomie gruntu mogą przechwytywać sygnały przekazywane przez pobliską wieżę, a ponieważ mikrofale przemieszczają się w liniach prostych, a nie podążają za krzywizną ziemi, ostatecznie kończą w przestrzeni kosmicznej, gdzie odbiorniki satelitarne mogą je gromadzić. Trudność podsłuchującego polega na tym, że w dowolnej wieży mogą znajdować się tysiące takich sygnałów, w tym głosu i danych. Wybór interesujących jest wyzwaniem. Jednak przy wystarczającej mocy obliczeniowej takie sortowanie jest możliwe, podobnie jak w przypadku określonych strumieni wiadomości. Skuteczne przeciwdziałanie stanowi transmisja rozproszonego widma lub przeskok częstotliwości.

SIECI Z PRZEŁĄCZANIEM PAKIETÓW

Sieci z komutacją pakietów, w tym historyczne nośniki X.25, takie jak Telenet, Tymnet i Datapac, wykorzystywały dezasemblery asemblerów pakietów (PAD) do grupowania danych w pakiety zaadresowane ze źródła do miejsca docelowego. Jeśli dane przesyłane są zwykłymi liniami telefonicznymi w celu dotarcia do sieci, przechwycenie może nastąpić w dowolnym miejscu wzdłuż tych segmentów łącza komunikacyjnego. Jednak gdy dane zostały podzielone na pakiety (po stronie klienta lub po stronie sieci), podsłuchiwacze mieli trudności ze zrozumieniem strumienia danych

POŁĄCZENIE INTERNETOWE

Połączenia TCP / IP nie są trudniejsze niż jakikolwiek inny i przenoszą stale rosnący wachlarz danych, od ruchu w handlu elektronicznym po transmisje telewizyjne i komunikację głosową, przy czym te ostatnie korzystają z protokołu VoIP (Voice over Internet Protocol). O ile strumień danych nie jest szyfrowany, nie ma specjalnych przeszkód dla podsłuchów. Chociaż gwintowanie kabla światłowodowego wymaga bardziej specjalistycznego sprzętu niż gwintowanie kabli miedzianych, jest to możliwe.

PRZECHWYTYWANIE PAKIETÓW LAN

Sieci lokalne (LAN) są podobne do sieci z przełączaniem pakietów: oba protokoły sieciowe przesyłają informacje w dyskretnych pakietach, za pośrednictwem kabli lub fal radiowych. Każda paczka ma nagłówek zawierający adres nadawcy i adresata. Pakiety są przesyłane do wszystkich węzłów w segmencie sieci LAN. Zwykle węzeł ogranicza się do interpretacji tylko tych pakietów, które są przeznaczone tylko dla niego. Można jednak ustawić urządzenia w „tryb nieograniczony", zastępując to ograniczenie. Można tego dokonać za pomocą oprogramowania, które potajemnie przekształca urządzenie, takie jak stacja robocza użytkownika końcowego, w urządzenie nasłuchujące, przechwytując wszystkie pakiety docierające do tego węzła. Oczywiście administratorzy sieci mogą celowo utworzyć stację roboczą do przechwytywania pakietów w uzasadnionych celach, takich jak diagnozowanie wąskich gardeł w sieci. Możliwe jest również podłączenie do sieci specjalistycznego sprzętu zwanego monitorami LAN, z pozwoleniem lub bez, w uzasadnionych lub nielegalnych celach. Czasami nazywane snifferami sieciowymi, te urządzenia i programy różnią się od podstawowego darmowego oprogramowania do drogich pakietów komercyjnych, które mogą kosztować dziesiątki tysięcy dolarów za sieć z setkami węzłów. (Termin „sniffer", chociaż jest powszechnie używany, jest zastrzeżonym znakiem towarowym, jak Sniffer R, Network General Corporation.) Bardziej zaawansowane programy do wykrywania pakietów pozwalają użytkownikowi konfigurować profile do przechwytywania; na przykład operator może wybrać pakiety przesyłane między hostem a stacją roboczą administratora systemu. Takie programy umożliwiają obserwatorowi przeglądanie i

rejestrowanie wszystkiego, co widać i zrobiono na stacji roboczej, w tym loginów lub kluczy szyfrujących wysyłanych na serwer. Wykrywanie pakietów stanowi poważne zagrożenie dla poufności transmisji danych przez sieci LAN. Większość programów snifferów nie ogłasza swojej obecności w sieci. Chociaż przypadkowy obserwator może nie wiedzieć, że stacja robocza wykonuje sniffowanie, możliwe jest, w ramach środków zaradczych, skanowanie sieci w poszukiwaniu urządzeń podsłuchujących. Lepsza technologia wykrywania pakietów stale się poprawia, a ścisłe bezpieczeństwo fizyczne może być najlepszym ogólnym czynnikiem odstraszającym. Użytkownicy sieci LAN zaniepokojeni poufnością powinni korzystać z protokołów LAN, które zapewniają kompleksowe szyfrowanie strumienia danych lub produkty innych firm do szyfrowania poufnych plików przed wysłaniem ich przez sieć LAN. Routery, które izolują segmenty sieci LAN lub WAN (sieć rozległa), mogą pomóc ograniczyć narażenie na zagrożenie ze strony snifferów.

ŚWIATŁOWÓD

Choć kiedyś uważano, że światłowody są bezpieczne przed przechwyceniem, nowe rozwiązania szybko zniosły tę nadzieję. Atakujący może zdjąć włókno światłowodowe z zewnętrznej obudowy i zgiąć je w spinkę o promieniu kilku milimetrów (1/8 cala); z zakrętu wydostaje się wystarczająca ilość światła, aby powielić strumień danych. Cytował Bryan Betts, pisząc w PCWorld Thomas Meier, CEO szwajcarskiej firmy Infoguard. . . . [kto] zademonstrował tę technikę na światłowodzie prowadzącym połączenie telefoniczne VOIP przez Gigabit Ethernet. Część światłowodu z wnętrza skrzynki połączeniowej została zapętlona w fotodetektor zwany łącznikiem zgięcia, a połączenie zostało zarejestrowane, a następnie odtworzone na laptopie. „Ludzie twierdzą, że światłowód jest trudniejszy do zerwania niż miedź, ale jest odwrotnie - nie trzeba nawet przebijać izolacji, tak jak w przypadku miedzi" - powiedział Meier. „Możesz odczytać okładzinę światłowodu z utratą sygnału nawet o pół dB." Twierdził, że odpowiednie łączniki zginające można kupić z półki - lub w serwisie eBay - za kilkaset dolarów i podłączyć do dodatkowego światłowodu, który jest zwykle pozostawiony zwinięty w skrzynkach połączeniowych na potrzeby przyszłych połączeń. Dodał, że ryzyko nie jest wymyślone ani teoretyczne - w sieciach policyjnych w Holandii i Niemczech znaleziono krany optyczne, a FBI zbadało tę odkrytą w sieci Verizon w Stanach Zjednoczonych. Zaatakowano również sieci używane przez brytyjskie i francuskie firmy farmaceutyczne, prawdopodobnie do szpiegostwa przemysłowego, powiedział.

Na szczęście większość optycznych kabli przesyłowych przenosi setki lub tysiące włókien, co praktycznie uniemożliwia zlokalizowanie konkretnego kanału komunikacyjnego. (To samo nie dotyczy kabli światłowodowych używanych do zapewnienia łączności sieciowej w poszczególnych domach i biurach.) Sprzęt do konwersji sygnałów optycznych na użyteczne dane pozostaje kosztowny, zniechęcając do jego używania przez przypadkowych hakerów kryminalnych.

KOMUNIKACJA BEZPRZEWODOWA

Zaletą komunikacji kablowej jest ograniczenie dostępu do kanału przynajmniej teoretycznie widocznym połączeniom. Jednak szybki wzrost telekomunikacji bezprzewodowej w ostatnim dziesięcioleciu XX wieku i pierwszych latach dwudziestego pierwszego roku skierował rosnącą ilość informacji za pośrednictwem mediów transmisyjnych, w których dostęp - nawet nieautoryzowany - może być niewidoczny dla użytkowników i systemu administrator

TELEFONY BEZPRZEWODOWE

Znane również jako telefony bezprzewodowe, konwencjonalne telefony bezprzewodowe transmitują swoje sygnały, a ruch, który niosą, można wykryć z daleka. Starsze telefony bezprzewodowe były analogowe i podatne na podsłuch z takich podstawowych urządzeń, jak krótkofalówki i nianie. Dzieci czasami spacerowały po swoich podmiejskich dzielnicach z włączonym telefonem z takiego telefonu;

gdy odeszli wystarczająco daleko od domu, aby utracić sygnał, każdy nowy sygnał wybierania należał do sąsiada, który może być zdziwiony odkryciem połączenia z Antypodami na następnym rachunku telefonicznym. Dzisiejsze modele telefonów bezprzewodowych zwykle używają innego zestawu częstotliwości, takiego jak 2,4 gigaherca (GHz). Telefony te zazwyczaj wykorzystują technologię FHSS, aby utrudnić nieautoryzowane użytkowanie i utrudnić podsłuch. FHSS oznacza, że sygnały przeskakują z częstotliwości na częstotliwość w całym spektrum 2,4 GHz, co utrudnia stukanie ich sygnałów, ale w żadnym wypadku nie jest niemożliwe. Telefonów bezprzewodowych nie należy używać do poufnego przesyłania głosu lub danych, chyba że szyfrowanie jest włączone i aktywowane. Dodatkowym niebezpieczeństwem jest zawieszenie telefonu bezprzewodowego podczas rozmowy, ponieważ podstawa telefonu bezprzewodowego kontynuuje transmisję aż do wyłączenia

TELEFONY KOMÓRKOWE

Wczesne analogowe systemy komórkowe (mobilne) miały prywatność równą oczekiwaniom wykrzykiwania wiadomości przez megafon z dachu. Połączenia na takich telefonach były łatwo przechwytywane za pomocą skanerów zakupionych w lokalnych sklepach z elektroniką. Chociaż szyfrowanie jest możliwe w nowszych powszechnie używanych telefonach cyfrowych, szyfrowanie nie zawsze jest włączone ze względu na obciążenie, jakie nakłada na firmę przełączającą. Przed założeniem, że połączenia komórkowe są szyfrowane, skontaktuj się z operatorem. Należy również pamiętać, że chociaż cyfrowe połączenia telefoniczne są trudniejsze do przechwycenia niż analogowe, istnieje kwitnący czarny rynek urządzeń umożliwiających takie przechwytywanie. Z reguły poufne informacje nigdy nie powinny być przekazywane przez telefony komórkowe bez uprzedniego zaszyfrowania linii lub wiadomości. Phil Zimmermann, twórca Pretty Good Privacy (PGP, później GPG) na początku lat 90., utworzył w 2012 r. Nową usługę o nazwie Silent Circle, aby zapewnić swoim abonentom szyfrowaną telefonię i dostęp do Internetu.

SIECI BEZPRZEWODOWE

Coraz popularniejszy sposób łączenia komputerów z sieciami znanymi jako Wi-Fi stwarza wiele możliwości przechwytywania komunikacji. W tym kontekście „sieć bezprzewodowa" zazwyczaj oznacza sieć danych wykorzystującą standard 802.11, która występuje w różnych odmianach, takich jak 802.11b, 802.11g (często łącznie określana jako WiFi, co oznacza „Wireless Fidelity" i oznacza właściwie marka należąca do grupy handlowej WiFi Alliance). Zazwyczaj jest to rodzaj sieci lokalnej utworzonej przez podłączenie bezprzewodowego punktu dostępu do sieci Ethernet oraz karty lub adaptera Wi-Fi do każdego komputera. Większość komputerów przenośnych ma teraz wbudowany adapter WiFi. Te sieci WLAN lub bezprzewodowe sieci lokalne są stosunkowo tanie i łatwe do utworzenia, ponieważ nie wymagają okablowania sieciowego. To pomaga wyjaśnić, dlaczego w 2006 r. Sprzedano ponad 200 milionów urządzeń Wi-Fi, a ponad połowa wszystkich amerykańskich firm korzysta z sieci WLAN w pewnym stopniu od 2002 r. Jednak tanie sieci WLAN wiążą się z ukrytymi kosztami, a mianowicie bezpieczeństwem. Każda sieć WLAN z natury działa w trybie Loliplips. W pewnym sensie łatwość użycia wiąże się z łatwością nadużyć. Wszyscy nadają swój ruch w powietrze, skąd może go podsłuchać ktoś z odpowiednim zestawem uszu, uprawniony użytkownik lub haker kryminalny, ktoś szukający darmowej przepustowości lub kierowca wojenny. Prowadzenie pojazdów wojennych, praktyka jeżdżenia po mieście w celu znalezienia bezprzewodowych punktów dostępowych, jest hobby dla niektórych osób i prawdopodobnie nie jest nielegalna, chyba że odbywa się to w złych zamiarach - wiele komputerów przenośnych próbuje znaleźć bezprzewodowe punkty dostępowe przy każdym włączeniu - ale należy pamiętać, że przepisy różnią się w zależności od kraju. (Osoby rozważające prowadzenie wojny powinny sprawdzić status prawny w swoich jurysdykcjach).

Aby zostać kierowcą wojennym, wystarczy stary laptop, odpowiednia karta WiFi, trochę wolnego oprogramowania (np. NetStumbler) i pusty ziemniak Pringles -chip może być podłączony do karty WiFi jako antena zewnętrzna w celu zwiększenia odbioru. (Pringles może być opcjonalny, podobnie jak globalny system pozycjonowania do oznaczania lokalizacji punktów dostępu Wi-Fi). Jeśli będziesz jeździł z aktywowanym sprzętem, bez wątpienia odkryjesz wiele punktów dostępu zarówno w dzielnicach mieszkaniowych, jak i biznesowych. Jeśli nazwy punktów dostępu to np. „Linksys" lub „netgear", oznacza to, że właściciel sieci nie zmienił domyślnego identyfikatora zestawu usług (SSID), który zwykle jest marką dostępu bezprzewodowego punkt, nadaj dla całego świata, chyba że właściciel sieci wyłączy tę funkcję. Nazwą może być także osoba, miejsce lub firma, która pomaga kierowcom wojennym dowiedzieć się, do kogo oni się zwracają. (Jeden z autorów wykrył SCHS w pobliżu biur Sample County Health Services.) Program taki jak NetStumbler poinformuje również, czy sieć używa szyfrowania. Odsetek sieci bezprzewodowych korzystających z szyfrowania stale rośnie, ale jest to znacznie mniej niż 10 procent. Według ankiety przeprowadzonej przez AT&T pod koniec 2007 r. Co szósta mała firma w Ameryce, która korzysta z technologii bezprzewodowej, nie podjęła żadnych środków ostrożności przeciwko zagrożeniom bezprzewodowym, a jedna trzecia małych firm stwierdziła, że nie są zaniepokojone bezpieczeństwem danych bezprzewodowych. Oznacza to, że WiFi, czy to w domu, w biurze, czy w gorącym punkcie, stanowi znaczącą kategorię wycieku danych, a tym samym główną drogę penetracji systemów.

VAS ECK PHREAKING

Atak ten nazwano na cześć Wima Van Ecka, holenderskiego badacza elektroniki, który w 1985 roku udowodnił wielu bankom, że możliwe jest odczytanie informacji z ich lamp katodowych (CRT) w odległości prawie mili, przy użyciu stosunkowo prostej technologii. Ponieważ wiele rodzajów urządzeń elektronicznych emituje sygnały o częstotliwości radiowej, odbiorniki, które przechwytują te sygnały, mogą być używane do rekonstrukcji naciśnięć klawiszy, wyświetlania wideo i strumieni drukowania. Za pomocą prostych, niedrogich odbiorników szerokopasmowych przestępcy mogą wykrywać i wykorzystywać takie emisje z odległości kilkudziesięciu lub setek metrów (jardów). Ponieważ sygnały o częstotliwości radiowej łatwo przeciekają przez okna jednopanelowe, komputerów nigdy nie należy umieszczać w widocznym oknie na parterze (a na pewno nie patrzeć w okno!). Tłumiki, które uderzają w okno w nieregularnych odstępach czasu, można zainstalować w celu wyeliminowania takiego wycieku. Specjalne dwupanelowe okno z gazem obojętnym między szybami może również zmniejszyć ilość wycieków sygnałów. Inne środki zaradcze obejmują specjalne okładziny sprzętu, takiego jak komputery i drukarki, w celu osłabienia sygnałów rozgłoszeniowych. Na ochronę tę często wskazuje nazwa sklasyfikowanego standardu rządowego dotyczącego ochrony wrażliwych systemów wojskowych, TEMPEST. Chociaż TEMPEST był rzekomo sklasyfikowanym słowem kodowym na początku, obecnie jest czasami rozszerzany jako Standard przejściowej elektromagnetycznej emisji impulsów lub Materiał elektroniki telekomunikacyjnej chroniony przed emanującymi fałszywymi transmisjami. Sprzęt z certyfikatem TEMPEST kosztuje wiele razy więcej niż ten sam sprzęt bez okładziny TEMPEST. Tańszą alternatywą jest użycie specjalnego urządzenia emitującego szum elektromagnetyczny, który maskuje znaczące sygnały. Jeszcze innym podejściem do ochrony przed tym zagrożeniem jest lokalizowanie systemów w budynkach lub pomieszczeń w budynkach, które zostały zbudowane zgodnie ze standardami TEMPEST. Istnieją przepisy federalne dotyczące metod budowy wrażliwych obiektów z przedziałami informacyjnymi (SCIF), a testowanie w celu uzyskania oceny TEMPEST jest dość rygorystyczne. Środki te obejmują takie elementy, jak okładziny wszystkich ścian i sufitów, okładziny wszystkich kabli elektrycznych i sieciowych, drzwi wyłożone ołowiem i brak jakichkolwiek okien zewnętrznych.

PRZECHWYTYWANIE INFORMACJI LOGOWANIA

Przestępcy mogą przechwytywać kody identyfikacyjne i uwierzytelniające, wstawiając konie trojańskie do procesu logowania na hoście serwera oraz używając narzędzi makro do rejestrowania naciśnięć klawiszy w węźle klienta. Jednak dziś częściej wykorzystywane jest specjalnie napisane złośliwe oprogramowanie do przechwytywania naciśnięć klawiszy i przesyłania ich w odstępach czasu z powrotem do zdalnego systemu

TROJANY LOGOWANIA OPARTE NA HOŚCIE

Koń trojański to program, który wygląda na użyteczny, ale zawiera nieautoryzowany, nieudokumentowany kod dla nieautoryzowanych funkcji. Nazwa pochodzi od mitologii greckiej, w której Odyseusz (Ulisses po łacinie), zmęczony niekończącym się oblężeniem Troi, zniknął z pola widzenia, jakby on i jego wojownicy poddawali się, ale zostawił wielkiego drewnianego konia u bram miejskich. Zachwyceni tą wspaniałą ofertą pokoju Trojanie wciągnęły wielkiego konia do miasta. Podczas dzikich obchodów trojańskich tej nocy, żołnierze Odyseusza wysunęli się z brzucha pustego konia i wyszli i otworzyli bramy dla swojej armii. Grecy wymordowali wszystkich mieszkańców miasta, a wojna trojańska dobiegła końca. W lutym 1994 r. Centrum Koordynacji Zespołu Reagowania Komputerowego (CERT-CC) na Uniwersytecie Carnegie Mellon w Pittsburghu wydało ostrzeżenie, że hakerzy kryminalni wprowadzili programy logowania koni trojańskich do setek systemów UNIX w Internecie. Trojan przechwytywał pierwsze 128 bajtów każdego logowania i zapisywał je w pliku dziennika, który został później odczytany przez przestępców. Ta sztuczka naruszyła około 10 000 identyfikatorów logowania. Kod trojana może być zainstalowany na komputerze lub terminalu używanym przez kilka osób (np. na terminalu mainframe w latach 70. lub w kafejce internetowej), aby gdy ktoś wprowadził identyfikator użytkownika i hasło do logowania, kontrolowany przez system przez trojana - wyświetla komunikat „Nieprawidłowe hasło, spróbuj ponownie”, a użytkownik to robi. Tym razem logowanie zostanie zaakceptowane. Ofiara kontynuuje pracę, nieświadoma, że dzieje się coś niezwykłego. Zainstalowany wcześniej trojan symulował normalną procedurę logowania, wyświetlając pozory oczekiwanego ekranu i okna dialogowego. Gdy ofiara wprowadzi hasło, trojan zapisuje dane uwierzytelniające do pliku, a następnie wyświetla mylący komunikat o błędzie. Program fałszowania kończy się, a zwykły program jest gotowy do logowania. Taki przypadek miał miejsce w kwietniu 1993 r. na przedmieściach Hartford w stanie Connecticut. Kupujący zauważyli w swoich centrach handlowych nowy bankomat (ATM). Początkowo urządzenie wydawało się działać poprawnie, wypłacając kilkaset dolarów użytkownikom kart bankowych na żądanie. Szybko zmienił się w bardziej złowieszczy tryb. Użytkownicy wkładali swoje karty bankowe i jak zwykle odpowiadali na żądanie osobistych numerów identyfikacyjnych (PIN). W tym momencie nowy bankomat wyświetli komunikat informujący o usterce i sugerujący, że użytkownik spróbuje skorzystać z sąsiedniej maszyny bankowej. Większość ludzi nic o tym nie myślało, ale w końcu ktoś zdał sobie sprawę, że bankomat nie wyświetlał zwykłego wskaźnika „Porządku” po tych rzekomych błędach. Ponadto banki zaczęły otrzymywać skargi na wysyp oszustw związanych z kartami bankowymi w najbliższej okolicy. Śledczy odkryli, że bankomat nie miał połączenia z żadnym znanym bankiem - że został zakupiony jako używany wraz ze sprzętem do produkcji kart bankowych. Bankomat był sfałszowany; gromadził jedynie identyfikator użytkownika i kod PIN każdej ofiary do późniejszego odebrania przez przestępców, którzy zainstalowali go bez pozwolenia w centrum handlowym. Przestępcy zostali złapani po kradzieży około 100 000 USD w ciągu czterech tygodni przy użyciu fałszywych kart bankowych.

REJESTROWANIE NACIŚNIĘĆ KLAWISZY

Kolejnym zagrożeniem dla kodów identyfikacyjnych i uwierzytelniających jest możliwość rejestrowania naciśnięć klawiszy w celu późniejszego odtwarzania lub edycji. Większość programów do edycji tekstów udostępnia funkcje makr, tak nazwane ze względu na ich zdolność do przechowywania i wyprowadzania wielu naciśnięć klawiszy, takich jak pisanie tekstu na płycie, za jednym naciśnięciem

klawisza. Bardziej wyrafinowane programy rezydentne (TSR) mogą rejestrować sekwencje poleceń i czasami są wykorzystywane do demonstrowania oprogramowania lub do automatyzacji testów zapewnienia jakości. Tej technologii można także używać do oczekiwania na stacji roboczej i rejestrowania wszystkiego, co użytkownik robi za pomocą myszy i pisania za pomocą klawiatury; takie programy są czasami nazywane rejestratorami naciśnięć klawiszy. Później przestępca może zbierać dane i wybierać kody logowania i inne cenne informacje. Istnieją również sprzętowe implementacje rejestrowania naciśnięć klawiszy. Jednym z nich jest małe urządzenie umieszczone między klawiaturą a komputerem, przechwytujące wpisane znaki i przechowujące je w nieulotnej pamięci, aż będzie można je odzyskać. Zdecydowanie najczęstszą formą rejestrowania naciśnięć klawiszy jest zaczepianie działających mechanizmów systemu zapewniających funkcjonalność klawiatury. Odbywa się to w oprogramowaniu. Istnieje wiele specyficznych technik technicznych umożliwiających przeprowadzenie procesu zaczepiania w zależności od systemu operacyjnego i sprzętu. Czasami oprogramowanie używane do rejestrowania naciśnięć klawiszy jest samodzielne, ale często jest częścią większego oprogramowania, które zapewnia również funkcje C2 (dowodzenia i kontroli). Często zdarza się, że funkcja rejestrowania naciśnięć klawiszy jest częścią rootkita, aby uniknąć wykrycia. Możliwe jest pokonanie próby ponownego użycia i nadużycia poświadczeń logowania przechwyconych dowolną z tych metod, przechodząc na hasła jednorazowe generowane przez mikroprocesory. Hasła jednorazowe zostały omówione w rozdziale 28 niniejszego podręcznika. Jednak, zarówno rejestratory kluczy, jak i trojany można wdrożyć, aby uzyskać nieautoryzowany dostęp do danych bez uciekania się do ponownego użycia haseł.

NARUSZENIE KONTROLI DOSTĘPU

Przestępcy i szpiedzy wykorzystują dwie szerokie kategorie ataków technicznych, aby wydedukować dostęp do numerów telefonów, identyfikatorów użytkowników i haseł: ataki brutalnej siły i inteligentne zgadywanie. Ponadto istnieją sposoby manipulowania ludźmi w celu ujawnienia ich kodów dostępu; techniki te zostały omówione w części poświęconej inżynierii społecznej.

ATAKI BRUTE-FORCE

Ataki typu brute-force polegają na użyciu potężnych komputerów do wypróbowania wszystkich możliwych kodów w celu zlokalizowania poprawnych. Brutalna siła jest stosowana do lokalizowania modemów, punktów dostępu do sieci, wrażliwych serwerów internetowych, identyfikatorów użytkowników i haseł.

WYBIERANIE DEMONICZNE (WOJENNE)

Pomimo hurtowego przenoszenia transmisji danych do sieci TCP / IP i Internetu modemy na telefonicznych liniach telefonicznych pozostają powszechnym, a czasem zapomnianym, zewnętrznym sposobem dostępu do systemu. Numery telefonów dowolnych modemów podłączonych do hostów lub serwerów lub inteligentnych urządzeń peryferyjnych sieci, takich jak wysokiej klasy drukarki laserowe, są wrażliwe i nie powinny być wysyłane ani nadawane. Demoniczne dialery to programy, które mogą wypróbować każdy numer telefonu w zakresie liczbowym i zarejestrować, czy jest odpowiedź głosowa, linia faksu, operator modemu, czy nie. Kiedy telefony dzwonią po całym biurze w kolejności numerycznej, jeden po drugim, a kiedy nie ma nikogo na linii, jeśli telefon zostanie odebrany, jest to niewątpliwie praca kogoś, kto używa demonicznego dialera. Oczywiście dobre oprogramowanie do wybierania demonów uzyskuje kolejno dostęp do numerów z zakresu docelowego. Podczas rozkwitu faksów niektórzy młodzi ludzie „w nocy” prowadzili całą hodowlę centrów telefonicznych, a następnie sprzedawali numery faksu za 1 dolara

WYCZERPUJĄCE WYSZUKIWANIE

To samo podejście, co wybieranie demonów, może znaleźć identyfikatory i hasła użytkowników po nawiązaniu połączenia. Atakujący używa programu, który cyklicznie przechodzi przez wszystkie możliwe identyfikatory użytkowników i hasła oraz rejestruje udane próby. Czas wymagany na ten atak zależy od dwóch czynników:

1. Obszar klawiszy dla kodów logowania

2. Maksymalna dopuszczalna prędkość próby logowania

W dzisiejszym środowisku technicznym każdy niedrogi komputer może generować kody logowania znacznie szybciej niż hosty zezwalają na próby logowania. Szybkość procesora nie jest już czynnikiem ograniczającym tempo. Pamiętaj, że ten rodzaj próby „odgadnięcia" haseł różni się od łamania haseł, opisanego w innym miejscu, który działa na przechwyconych lub skradzionych kopiach zaszyfrowanych plików haseł.

KEYSPACE

Jak omówiono wcześniej, przestrzeń klucza dla kodu to maksymalna liczba możliwych ciągów, które spełniają reguły ograniczeń logowania. Na przykład, jeśli hasła użytkownika składają się z dokładnie sześciu wielkich lub małych liter lub cyfr, a w haśle rozróżniana jest wielkość liter (tzn. Wielkie litery są odróżniane od małych), całkowita liczba możliwych kombinacji takich haseł jest obliczana w następujący sposób:

* Jest 10 cyfr i 52 wielkich lub małych liter (alfabetu angielskiego) = 62 możliwe kody dla dowolnej z sześciu pozycji.

* Jeśli nie ma ograniczeń dotyczących powtarzania, ciąg n znaków, które należy pobrać z listy r możliwości dla każdej pozycji, wygeneruje rn możliwych kombinacji.

* Zatem w naszym przykładzie istnieje 62^6 możliwych sekwencji 62 kodów pobranych w grupach po sześć = 56 800 235 584 (ponad 56 miliardów) możliwych kodów logowania.

Jeśli istnieją ograniczenia, przestrzeń na klucze zostanie odpowiednio zmniejszona. Na przykład, jeśli pierwszy znak hasła o długości sześć musi być wielką literą zamiast dowolnej litery lub cyfry, istnieje tylko 26 możliwości dla tej pozycji zamiast 62, zmniejszając w ten sposób całkowitą przestrzeń klawiszy do 26×62^5 = 23 819 453 632 (więcej ponad 23 miliardy) możliwości.

TĘCZOWE TABELE

Kryptoanalitycy (w tym kryptoanalityk przestępca) mogą generować wszystkie możliwe skróty jednokierunkowe dla przestrzeni kluczy dowolnej reguły hasła; w ten sposób można przyspieszyć pękanie metodą brute-force. Są nawet strony internetowe, które dystrybuują takie tabele swobodnie.

SZYBKOŚĆ LOGOWANIA

Generowanie kodów logowania nie jest trudne. Największą barierą dla ataków z użyciem siły brute-force jest przerwanie logowania za każdym razem, gdy host wykryje błąd. Większość systemów operacyjnych i monitorów bezpieczeństwa zezwala administratorowi na zdefiniowanie dwóch typów opóźnień logowania i następujące błędy:

1. Zwykle krótkie opóźnienie po każdej nieudanej próbie wprowadzenia poprawnego hasła

2. Zwykle duże opóźnienie po kilku nieudanych próbach logowania

Załóżmy, że każde wprowadzone błędne hasło powoduje opóźnienie o 1/10 sekundy przed wprowadzeniem następnego hasła; następnie w naszym przykładzie obejmującym sześć powtarzalnych wielkich lub małych liter lub cyfr zajęłoby to 5680 023 558 sekund = 1577 784 godzin - 180 lat, aby wypróbować każdą możliwość. Załóżmy ponadto, że po każdej piątej nieudanej próbie logowania system miał dezaktywować identyfikator użytkownika lub port modemu na trzy minuty. Taka ingerencja wydłużyłaby teoretyczny czas wyczerpującego ataku brutalnej siły do około 650 lat. Czy menedżer bezpieczeństwa powinien całkowicie dezaktywować identyfikator, jeśli jest atakowany?

Jeśli identyfikator zostanie dezaktywowany, dopóki użytkownik nie wezwie pomocy, identyfikatory użytkownika będą narażone na dezaktywację przez złośliwych hakerów. Atakujący muszą jedynie podać złe hasło kilka razy z rzędu, a niczego niepodejrzewający prawowity użytkownik zostanie zablokowany w systemie do odwołania. Powszechny atak na wiele identyfikatorów użytkowników może uniemożliwić system większości użytkowników. Taki wynik byłby atakiem typu „odmowa usługi". Czy port należy dezaktywować? Jeśli jest tylko kilka portów, zamknięcie ich spowoduje, że system będzie niedostępny dla legalnych użytkowników. Ta drastyczna reakcja może być nieodpowiednia - w rzeczywistości może zaspokoić intencje hakerów kryminalnych. Krótkie opóźnienie, może kilka minut, prawdopodobnie wystarczyłoby, aby zniechęcić do ataków siłowych. We wszystkich tych przykładach ilustracje oparte były na wyczerpujących atakach (tj. wypróbowaniu każdej możliwości). Jeśli jednak hasła lub inne kody zostaną wybrane losowo, prawidłowe kody zostaną równomiernie rozmieszczone w przestrzeni klawiszy. Średnio zatem, zgodnie z zasadą statystyki zwaną Centralnym Twierdzeniem Granicznym, wyszukiwania metodą brutalnej siły będą musiały przeszukać połowę przestrzeni kluczowej. W przypadku dużych obszarów kluczy różnica między bardzo długim a połową bardzo długiego czasu będzie w praktyce nieistotna (np. 325 lat nie różni się znacząco od 650 lat, jeśli wszyscy zainteresowani zginą przed złamaniem kodu).

OCZYSZCZANIE PAMIĘCI O DOSTĘPIE SWOBODNYM.

Nie wszystkie ataki pochodzą od zewnętrznych agentów. Przestępcy posiadający fizyczny dostęp do stacji roboczych, złośliwego oprogramowania lub autoryzowani użytkownicy, którzy mogą korzystać z uprzywilejowanych narzędzi do odczytu pamięci głównej, mogą przeszukiwać obszary pamięci w celu uzyskania poufnych informacji, takich jak identyfikatory logowania i hasła. Na stacji roboczej używającej emulatora terminala do pracy z hostem zakończenie sesji niekoniecznie zwalnia emulator. Wiele emulatorów ma konfigurowalny bufor wyświetlania ekranu, czasem tysiące linii. Po tym, jak autoryzowany użytkownik wyloguje się i opuści terminal, zmiatacz może odczytać wiele stron aktywności, czasem włączając poufne informacje, a nawet kody logowania. Jednak hasła są zwykle niewidoczne i dlatego nie są zagrożone. Jeśli stacja robocza jest częścią systemu klient / serwer, aplikacja sterująca dostępem może pozostawić pozostałości w pamięci o dostępie swobodnym (RAM). Edytor RAM, łatwo dostępny jako część pakietów narzędzi, może przechwytywać i dekodować takie obszary, jak bufory plików lub bufory wejścia / wyjścia (I / O) dla portów komunikacyjnych. Ponowne uruchomienie stacji roboczej po zakończeniu komunikacji zapobiega oczyszczaniu pamięci RAM przez ponowne zainicjowanie pamięci.

OCZYSZCZANIE PLIKÓW PAMIĘCI PODRĘCZNEJ

Tę samą zasadę można zastosować do różnych plików pamięci podręcznej i wymiany utworzonych przez system operacyjny. Pliki pamięci podręcznej służą do tego, aby często używane dane były łatwo dostępne dla aplikacji. Pliki wymiany przechowują dane i kod, które są przenoszone z pamięci na dysk, gdy pamięć jest pełna. Niektóre systemy operacyjne również tworzą pliki hibernacji, zapisując pamięć na dysku tuż przed wyłączeniem zasilania, a tym samym umożliwiając szybkie wznowienie pracy po włączeniu systemu. Systemy operacyjne mogą również zapewniać automatycznie zapisywane pliki

odzyskiwania, które umożliwiają przywracanie danych po błędzie systemowym. Wszystkie z nich można wydobywać w celu uzyskania poświadczeń systemowych, a także innych cennych danych.

OCZYSZCZNIE PLIKÓW HISTORII ONLINE/ODZYSKIWAIE ZAPISANYCH HASEŁ

Nowsza odmiana na ten temat podejście do oczyszczania polega na sprawdzeniu plików utworzonych przez przeglądarki internetowe. Niekiedy zawierają one nie tylko strony przeglądane przez użytkownika, ale także dane uwierzytelniające wprowadzone w celu uzyskania dostępu do tych stron. Wiele aplikacji przechowuje hasła użytkowników lokalnie. Większość aplikacji próbuje zabezpieczyć te hasła, niestety rzadko są one przechowywane przy użyciu odpowiednich metod szyfrowania. Złośliwe oprogramowanie odzyskuje przechowywane hasła i przesyła je na zdalne serwery w celu ich zebrania przez osoby atakujące

INTELIGENTNE ZGADYWANIE

Użytkownicy rzadko wybierają losowe hasła. Znacznie częściej hasła są wybierane z podzbioru wszystkich możliwych ciągów. Zamiast ślepo klikać we wszystkich możliwych sekwencjach w przestrzeni kluczowej, atakujący może spróbować zmniejszyć efektywną przestrzeń kluczową, zgadując bardziej prawdopodobne wybory. Prawdopodobne wybory obejmują hasła kanoniczne, złe hasła i słowa wybrane ze słownika. Sprzęt i oprogramowanie często pochodzą z fabryki lub od razu po wyjęciu z pudełka, a identyfikatory i hasła użytkowników są takie same dla wszystkich systemów i użytkowników. Na przykład punkty dostępu bezprzewodowego i routery mają domyślne identyfikatory użytkownika, gdy są wysyłane z fabryki. Oczywiście te identyfikatory użytkowników są skonfigurowane z tym samym hasłem. (Na przykład „admin" na urządzeniach routerów bezprzewodowych Linksys.) Takie systemy zawsze zawierają instrukcje zmiany haseł, ale zbyt często administratorzy i użytkownicy zaniedbują to. Przestępcy są zaznajomieni z ustawieniami fabrycznymi - z których większość jest łatwo wykrywalna przez Google - i wykorzystują je do penetracji systemów. Prosta procedura zmiany wszystkich kanonicznych haseł uniemożliwia hakerom łatwy dostęp do systemów i oprogramowania.

KRADZIEŻ

Każdy element systemu komputerowego ma potencjalną wartość dla złodzieja. Dlatego należy zabezpieczyć każdy element, w tym sprzęt, oprogramowanie, nośniki, pliki, dokumentację i wydruki

OCZYSZCZANIE DANYCH

Hakerzy kryminalni nie mają skrupułów w kwestii korzystania z cudzej własności, gdy wchodzą do systemów komputerowych; w ogóle nie mają nic wspólnego z używaniem śmieci innych ludzi. Termin „oczyszczanie danych" opisuje proces uzyskiwania informacji ze źródeł wyrzucanych. Być może najbardziej znanym jest nurkowanie Dumpster , sortowanie według wszystkiego, co organizacja odrzuca. Wydruki, dyski CD-ROM, taśmy i inne różnorodne nośniki danych często kończą się w pojemnikach na śmieci, gdzie są łatwo dostępne dla nurków Dumpster po godzinach. W niektórych rejonach, jeśli ktoś odwiedza biuro lub park przemysłowy w nocy, można zobaczyć, jak w środku kręci się pół tuzina ludzi, czasem łobuzerskich w Dumpsters . Hakerzy kryminalni używają informacji bezmyślnie odrzucanych przez naiwnych pracowników biurowych jako źródła procedur, słownictwo i imiona, które mogą pomóc im podszywać się pod pracowników przez telefon lub nawet osobiście. Klasycznym przykładem jest odrzucony wewnętrzny spis telefonów, który może dostarczyć socjologowi cennych danych do wykorzystania podczas wykonywania połączeń z pracownikami. Pracownik, który waha się spełnić fałszywe żądanie atakującego przez telefon, może zostać przekonany, jeśli atakujący powie coś w stylu „Rozumiem twoje wahanie; jeśli czujesz się bardziej komfortowo, możesz zadzwonić z powrotem pod numerem wewnętrznym 2645. "Jeśli 2645 jest uzasadnionym wewnętrznym

numerem wewnętrznym, dzwoniący zyskuje znaczną wiarygodność. Oczywiście odpowiednio przeszkolony pracownik rozłączy się i zadzwoni pod numer 2645, a nie wybierze łatwą opcję i powie: „Myślę, że to w porządku, oto informacje, których chciałeś". Niektóre wydruki zawierają poufne informacje, które mogą prowadzić do wymuszenia lub penetracja systemu. Na przykład złodziej, który kradnie listę danych osobowych dotyczących pacjentów z zakażeniem HIV, może dręczyć ofiary i wyłudzać pieniądze. Każdy kawałek papieru lub inne media, które należy wyrzucić, należy ocenić pod kątem poufności. O ile informacje te nie są bezwartościowe dla wszystkich, pracownicy powinni zniszczyć papier przed usunięciem lub zorganizować wysłanie papieru do służby celnej w celu zniszczenia. To samo dotyczy płyt CD-ROM i innych mediów.

ZUŻYTE NOŚNIKI MAGNETYCZNE I OPTYCZNE

Wyrzucony papier stanowi zagrożenie; zużyte nośniki magnetyczne i optyczne są katastrofą. Wiele organizacji nie uczy pracowników, że zwykłe polecenia używane do usuwania plików nie usuwają całego ich śladu. Zarówno za pomocą programów narzędziowych, jak i samego systemu operacyjnego można zlokalizować oryginalne klastry plików i odtworzyć dowolną część oryginalnego pliku, która nie została jeszcze nadpisana. Kopie zapasowe taśm, dysków CD i DVD mogą zawierać cenne informacje na temat struktury bezpieczeństwa systemu. Na przykład w latach 70. i 80. kopie zapasowe systemu jednej marki minikomputera zawierały cały katalog wraz z każdym identyfikatorem użytkownika i hasłem widocznym na pierwszej taśmie. Za pomocą prostego narzędzia do kopiowania plików każdy użytkownik może je odczytać dane. Aby zniszczyć informacje na nośnikach magnetycznych, użytkownicy muszą kilkakrotnie zastąpić nośnik losowymi danymi lub fizycznie zniszczyć nośnik. Demagnetyzery są nieodpowiednie, chyba że spełniają specyfikacje wojskowe, ale takie jednostki zazwyczaj kosztują tysiące dolarów. Problem odczytu danych jest szczególnie kłopotliwy w przypadku odrzuconych dysków twardych lub uszkodzonych dysków twardych, które zostały naprawione lub podlegają specjalnemu odzyskiwaniu danych. Użytkownicy otrzymali działające, obciążone danymi dyski jako zamienniki własnych uszkodzonych jednostek. Czasami dyski zastępcze nawet nie zostały sformatowane; zawierają całe katalogi korespondencji, bazy danych klientów i zastrzeżone oprogramowanie. Ponieważ z definicji niemożliwe jest nadpisywanie danych na uszkodzonym dysku, specjaliści ds. bezpieczeństwa wojskowego rutynowo niszczą uszkodzone dyski twarde za pomocą palników oksyacetylenowych lub specjalnie zaprojektowanych szlifierek, które zmniejszają dyski twarde na małe fragmenty.

SZPIEGOWANIE

Niektóre techniki stosowane przez hakerów kryminalnych zostały pobrane bezpośrednio z powieści szpiegowskich. Na przykład interferometria laserowa może odtworzyć wzorce drgań z odbitych wiązek laserowych podczerwieni odbijanych od okien. Użytkownicy takiego sprzętu mogą słyszeć i nagrywać rozmowy w pokojach z zewnętrznymi oknami, które wibrują zgodnie z dźwiękiem w pomieszczeniu. Hakerzy ukradkiem kradną kody dostępu ludzi, obserwując ich palce, gdy uderzają w tajne sekwencje. Kiedy popularne były telefony płatne, surferzy przechwytywali kody kart telefonicznych, które sprzedają zorganizowanym grupom przestępczym. Kody mogą zostać skradzione przez zerknięcie przez ramię sąsiadów lub użycie lornetki, teleskopu i kamery wideo do śledzenia przycisków naciskanych przez ich ofiary. Surfowanie na ramionach może również występować w instalacjach. Na przykład większość użytkowników zamków z kluczem nie zwraca uwagi na widoczność swoich palców. Za każdym razem, gdy wprowadzasz kod, użytkownicy powinni unikać obserwacji przez osoby nieupoważnione. W miejscach publicznych użytkownicy powinni stać blisko klawiatury. W instalacjach stacjonarnych zarządcy obiektów powinni zakrywać klawiatury z nieprzezroczystymi rękawami, umożliwiając swobodny dostęp, ale ukrywając szczegóły kodów dostępu. Przestępcy są biegli w surfowaniu zarówno w sieci przewodowej, jak i bezprzewodowej podróżując po mieście w warunkach

wojennych lub spędzając czas w bogatym w cele otoczeniu, takim jak lotnisko, dworzec kolejowy, kawiarnia lub lobby hotelu. Szczególnym typem połączenia przewodowego, z którego należy korzystać ostrożnie, jest szerokopasmowe połączenie z pokojem gościnnym oferowane przez wiele hoteli. Zbyt często są one konfigurowane bez odpowiednich środków bezpieczeństwa, umożliwiając ciekawemu lub skłonnemu kryminalnie gościowi zlokalizowanie maszyn należących do innych gości (czasami po prostu poprzez kliknięcie ikony Otoczenie sieciowe w Eksploratorze Windows). Pracownicy powinni zostać pouczeni, aby nie podłączać laptopów firmowych do takich połączeń, chyba że mają odpowiednio skonfigurowaną zaporę ogniową i są włączone oraz korzystają z wirtualnej sieci prywatnej (VPN) w celu uzyskania dostępu do systemów korporacyjnych

TESTY PENETRACYJNE , ZESTAWY NARZĘDZI I TECHNIKI

Weryfikacja i poprawa bezpieczeństwa systemów poprzez próbę ich penetracji jest ugruntowaną praktyką wśród specjalistów ds. bezpieczeństwa i administratorów systemów. Jednak chociaż niektórzy ćwiczyli tę technikę wcześniej, nie była ona otwarcie omawiana przed 1993 r. W tym roku Dan Farmer i Wietse Venema opublikowali pionierski artykuł zatytułowany „Poprawa bezpieczeństwa Twojej witryny poprzez włamanie się na nią". W tym artykule pojęcie oceny bezpieczeństwa systemu poprzez badanie systemu oczami potencjalnego intruza. Farmer i Venema wykazali, że skanowanie w poszukiwaniu pozornie nieszkodliwych usług sieciowych może ujawnić poważne słabości dowolnego systemu. Przed opublikowaniem tego ważnego dokumentu wielu administratorów systemu nie było świadomych zakresu luk w zabezpieczeniach systemów. Farmer i Venema wydali następnie program do testowania sieci o nazwie SATAN (Security Analysis Tool for Auditing Networks). Specjaliści ds. Bezpieczeństwa i administratorzy systemu chwalili i byli rozgniewani przez program. Niektórzy administratorzy systemu dopingowali dostępność narzędzia typu „wszystko w jednym", które ujawniło luki w zabezpieczeniach, ale ich nie wykorzystało. Inni kwestionowali motywy autorów dotyczące wydania bezpłatnego i łatwo dostępnego narzędzia, które hakerzy mogliby wykorzystać do atakowania sieci. Podczas gdy trwała debata, zarówno administratorzy systemu, jak i hakerzy zaczęli wykorzystywać SATAN do przesłuchiwania sieci.

WSPÓLNE NARZĘDZIA

Od tego czasu pojawiły się setki zestawów narzędzi penetracyjnych; są one powszechnie nazywane skanerami. Dziś można znaleźć niezliczone bezpłatne narzędzia lub zainwestować w jedno z komercyjnych narzędzi. Skanery różnią się złożonością i niezawodnością. Jednak większość narzędzi wykorzystuje te same podstawowe funkcje do testowania sieci: odpytuje porty na komputerach docelowych i rejestruje odpowiedź lub brak odpowiedzi. Użyte we właściwy sposób narzędzia te mogą być skuteczne w wykrywaniu i rejestrowaniu ogromnych ilości danych o sieci systemów komputerowych i ujawnianiu luk bezpieczeństwa w sieci. Wiele pakietów skanerów zawiera również aplikacje do wykrywania pakietów, opisane wcześniej. Administratorzy mogą wykorzystać te informacje do zmniejszenia liczby zagrożonych systemów. W dowolnym teście penetracyjnym można zastosować szeroką gamę podstawowych narzędzi sieciowych. Narzędzia te mogą obejmować zwykłe programy, takie jak PING, FINGER, TRACEROUTE i NSLOOKUP. Jednak najpoważniejsze narzędzia penetracyjne wykorzystują narzędzie do automatycznej analizy podatności składające się z szeregu zapytań dotyczących portów i bazy danych znanych luk. Niektóre narzędzia próbują również wykorzystać zidentyfikowane luki w celu wyeliminowania fałszywych alarmów. Po znalezieniu luk w zabezpieczeniach niezwykle łatwo jest uzyskać „exploity" lub programy, za pomocą których można przeprowadzić atak przeciwko podatnym maszynom. Wszystkie narzędzia wykorzystują podstawowe operacje pakietu protokołów TCP. Chociaż te protokoły będą działać na różnych numerach portów, wszystkie mają wspólną strukturę trójstronnego uzgadniania. Wszystkie protokoły TCP szukają próby połączenia (połączenia), synchronizacji i wymiany potwierdzeń (SYN / ACK), różnych warunków (FLAGS)

i żądania zamknięcia portu (FIN). Dlatego działanie skanerów portów jest dość podobne. Próbują znaleźć otwarte lub nasłuchujące porty na komputerze, poprosić o połączenie, a następnie zapisać wyniki w pliku, który ma zostać porównany z wewnętrzną bazą danych. Skaner wyświetli wyniki skanowania, wyświetlając listę otwartych portów i usług, które wydają się być uruchomione. W tym momencie różne programy różnią się. Niektórzy próbują dogłębnej analizy możliwych luk w zabezpieczeniach związanych z portami i usługami, wraz z odpowiednimi środkami bezpieczeństwa, aby je zabezpieczyć. Bardziej złośliwe skanery zawierają również zautomatyzowane skrypty do wykorzystania w ten sposób ujawnionych luk. Z darmowych narzędzi Nessus, Netcat i nmap są prawdopodobnie najlepiej znane, chociaż zawsze wydaje się, że zarówno hakerzy, jak i administratorzy systemu mają nowy smak miesiąca. SATAN jest nadal dostępny, podobnie jak jego spin-offy, SAINT i SARA. Do korzystania z tych narzędzi wymagana jest spora ilość umiejętności, ponieważ są one dość wyrafinowane, a niektóre skany mogą przeciążać system i powodować zawieszanie się lub awarię.

TYPOWE SKANY

Jak wspomniano wcześniej, większość dostępnych skanerów / snifferów będzie przebiegać według tych samych podstawowych procedur w celu stworzenia obrazu maszyny jako całości. Celem jest ustalenie, co działa na komputerze i jaka jest jego rola w sieci. Kolejne sekcje opisują najbardziej podstawowe skany i ich wyniki.

TCP CONNECT

Jest to najbardziej podstawowa forma skanowania TCP. To wywołanie systemowe jest dostarczane przez system operacyjny. Jeśli port nasłuchuje, próba połączenia będzie kontynuowana. To skanowanie nie wymaga uprawnień administratora ani administratora. Jednak skanowanie to jest łatwe do wykrycia, ponieważ wiele żądań połączenia i zakończenia zostanie wyświetlonych w dziennikach systemowych hosta.

TCP SYN

To skanowanie nie otwiera pełnego połączenia i jest czasami określane jako skanowanie na wpół otwarte, ponieważ pełny hand shake nigdy się nie kończy. Skanowanie SYN rozpoczyna się od wysłania pakietu SYN. Wszelkie otwarte porty powinny odpowiadać SYN | ACK. Jednak skaner wysyła RST (reset) zamiast ACK, co kończy połączenie. Mniej systemów rejestruje ten typ skanowania. Porty, które są zamknięte, zareagują

SKANOWANIE STEALTH

Skanowanie ukryte, nazywane również skanowaniem Stealth FIN, Xmas Tree lub Null, jest używane, ponieważ niektóre zapory ogniowe i systemy wykrywania włamań obserwują SYN do ograniczonych portów. Skanowanie ukryte próbuje ominąć te systemy bez tworzenia dziennika próby. Skanowanie polega na tym, że zamknięte porty powinny odpowiedzieć na żądanie za pomocą RST, a otwarte porty powinny po prostu upuścić pakiet bez rejestrowania próby.

SKANOWANIE UDP

Istnieje wiele popularnych luk do wykorzystania w protokole UDP (User Datagram Protocol), takich jak dziura rpcbind lub program trojański, taki jak Back Orifice cDc, który instaluje się na porcie UDP. Skaner wyśle 0-bajtowy pakiet UDP do każdego portu. Jeśli host zwróci komunikat „Port nieosiągalny”, port ten zostanie uznany za zamknięty. Ta metoda może być czasochłonna, ponieważ większość hostów UNIX ogranicza częstość błędów protokołu ICMP (Internet Control Message Protocol). Niektóre

skanery wykrywają dopuszczalną szybkość w systemach UNIX i spowalniają skanowanie, aby nie zalać celu wiadomościami.

SKANOWANIE PROTOKOŁU IP

Ta metoda służy do określania, które protokoły internetowe są obsługiwane na hoście. Surowe pakiety IP bez nagłówka protokołu są wysyłane do każdego określonego protokołu na maszynie docelowej. Jeśli zostanie odebrany nieosiągalny komunikat ICMP, protokół nie jest używany. W przeciwnym razie zakładano, że jest otwarty. Niektóre hosty (AIX, HP-UX, Digital UNIX) i zapory mogą nie wysyłać wiadomości nieosiągalnych dla protokołu, więc wszystkie protokoły wydają się być otwarte

ACK SAN

Ta zaawansowana metoda jest zwykle używana do mapowania zestawów reguł zapory. W szczególności może pomóc ustalić, czy zapora sieciowa jest stateczna, czy to tylko prosty filtr pakietów, który blokuje przychodzące pakiety SYN. Ten typ skanowania wysyła pakiet ACK z losowo wyglądającymi numerami potwierdzeń / sekwencji do określonych portów. Jeśli RST powróci, port jest klasyfikowany jako „niefiltrowany". Jeśli nic nie wraca lub jeśli ICMP jest nieosiągalny, port jest klasyfikowany jako „filtrowany".

SKANOWANIE RPC

Ta metoda otwiera wszystkie znalezione porty TCP / UDP, a następnie zalewa je poleceniami NULL programu SunRPC, próbując ustalić, czy są to porty RPC, a jeśli tak, to jaki program i numer wersji zwracają.

FTP BOUNCE

To skanowanie wygląda na serwer proxy FTP w sieci (lub zaufanej domenie). Może w końcu połączyć się z serwerem FTP za zaporą ogniową. Po znalezieniu serwera FTP skanowanie portów normalnie zablokowanych z zewnątrz można wykonać z wewnętrznego serwera FTP. Oczywiście czytanie i pisanie do katalogów można również sprawdzić na tym serwerze.

PING SWEEPA

Ten skan wykorzystuje Ping (żądanie echa ICMP), aby znaleźć hosty, które działają. Może także szukać adresów rozgłaszanych przez podsieć w sieci. Są to adresy IP, które można uzyskać zewnętrznie. Przeszukiwania pingów często służą do „mapowania" sieci jako całości.

SYSTEM OPERACYJNY ODCISKU PALCA

Ponieważ wiele luk w zabezpieczeniach zależy od systemu operacyjnego hosta, skanowanie to próbuje określić, który system operacyjny jest uruchomiony, na podstawie wielu przypuszczeń. Wykorzystuje różne techniki w celu wykrycia subtelności w stosie sieciowym systemu operacyjnego (OS) skanowanych komputerów. Zebrane dane są wykorzystywane do utworzenia „odcisku palca", który jest porównywany z bazą danych skanerów znanych odcisków palców. W przypadku znalezienia nieznanego odcisku palca osoby atakujące mogą sprawdzić witryny internetowe i grupy dyskusyjne, w których informacje o odciskach palców są przedmiotem swobodnego handlu, aby dowiedzieć się, jaki może być konkretny system operacyjny. Po zidentyfikowaniu systemu operacyjnego można łatwo znaleźć exploity za pomocą wyszukiwarki w Internecie. Pobieranie odcisków palców w systemie operacyjnym nie jest konieczne, jeśli system operacyjny można wykryć czytając banery. Na przykład, jeśli ktoś ma telnet na maszynę, odpowiedź może wyglądać następująco:

badgny~> telnet abcd.efg.com

Próbuję 163.143.103.12…

Połączony z abcd.efg.com

Znakiem ucieczki jest „ˆ]’.

HP-UX hpux B.10.01 A 9000/715 (ttyp2)

Zaloguj sie:

Baner, który był zawarty w domyślnej konfiguracji, po prostu wskazuje, że system operacyjny to HP-UX. Dobry administrator systemu wyłączy banery we wszystkich usługach, które je mają.

SKANOWANIE WSTECZNEJ TOŻSAMOŚCI

To skanowanie zwykle służy do sprawdzenia, czy serwer sieciowy w sieci działa jako root. Jeśli demon identd działa na komputerze docelowym, żądanie TCP Ident spowoduje, że demon zwróci nazwę użytkownika, który „jest właścicielem” procesu. Dlatego jeśli to żądanie zostanie wysłane do portu 80 (hex), a użytkownik zwrotny jest rootem, serwer ten może zostać użyty do ataku na system. To skanowanie wymaga pełnego połączenia TCP z danym portem, zanim zwróci nazwę użytkownika.

SKANOWANIE KONFIGURACJI WŁASNEGO PORTU

Steve Gibson z Gibson Research Corporation udostępnia darmowy skaner portów, który identyfikuje otwarte porty wśród pierwszych 1056 portów TCP w dowolnym systemie w ciągu mniej niż minuty. Dowolne otwarte port może być następnie kontrolowany przy użyciu odpowiedniego ustawienia zapory. W idealnym przypadku wszystkie porty na stacjach roboczych nie odpowiadają na polecenia ping.

PODSTAWOWE EXPLOITY

Korzystając z wyników programu skanującego, kolejnym logicznym krokiem dla hakerów będzie próba wykorzystania widocznych słabości systemu. Hakerzy próbują złamać komputer w sieci, pozwalając mu na uruchamianie programów lub procesów do woli na poziomie root. Gdy hakerzy „opanują” tę maszynę, możliwości są nieograniczone. Hakerzy mogą przeprowadzić atak na sieć z tej maszyny, zainstalować tylne drzwi do przyszłego użytku lub zainstalować konie trojańskie, aby zebrać więcej danych o użytkownikach. Wymienienie wszystkich dostępnych exploitów wykracza poza zakres tej sekcji . Po prostu jest ich zbyt wiele, a nowe pojawiają się każdego dnia. Liczba stron internetowych poświęconych hakowaniu jest ogromna. Jednak każdy administrator systemu powinien znać kilka podstawowych exploitów.

PRZEPEŁNIENIE BUFORA

Niewiele exploitów jest bardziej podstawowych lub bardziej rozpowszechnionych niż przepełnienia bufora, zwanych również przepełnieniami bufora. Bufor to obszar pamięci, w którym dane są tymczasowo przechowywane podczas przenoszenia z jednego miejsca do drugiego (np. Gdy program wymaga danych wejściowych z klawiatury, dane wejściowe są umieszczane w buforze przed przekazaniem do programu). Ponieważ zasoby obliczeniowe nie są nieograniczone, bufory mają zwykle stałą długość. O ile nie zostanie zachowane ostrożność w programowaniu, dane wejściowe dłuższe niż oczekiwano mogą przepełnić bufor z sąsiednich obszarów pamięci, powodując problemy z uszkodzeniem danych do nieprawidłowego zakończenia procesu. Możliwe skutki przepełnienia bufora są liczne. Bufor może przepełnić sąsiedni bufor i go uszkodzić. Sam warunek przepełnienia może wystarczyć, aby zawiesić proces. Skutki takiej awarii są często nieprzewidywalne i mogą skutkować rozszerzonym dostępem lub uprzywilejowaniem każdego, kto spowodował awarię. Przepełnienie

bufora właściwie spreparowane przez hakera może wstrzyknąć kod hakera do systemu. Przepełnienia bufora występują w aplikacjach oraz w podstawowych protokołach. Aplikacje otrzymujące dane wejściowe muszą zapewniać tymczasowe miejsce lub bufor dla tych danych. Jeśli dostarczonych zostanie więcej danych, niż się spodziewano, i nie przewiduje się ograniczenia wejściowego lub uporządkowanego reagowania na nadmiar wejściowy, mogą wystąpić błędy, powodujące awarie, zwiększony dostęp i tym podobne. Kluczem do wielu ataków przepełnienia bufora w sieciach jest fakt, że wiele protokołów nie potrafi odróżnić danych od kodu. Hakerzy starają się, aby ostatnia część danych zapisywana w obszarze przepełnienia była komendą lub fragmentem kodu, który wykona polecenie, tak jakby odpowiedź na żądanie wejściowe „Nazwa?" Była jak „Peter jak mój dziadek, który był pierwotnie z Rosji, ale podróżował po całym świecie, zanim się tu przeprowadził, a tak przy okazji, kiedy dotrzesz do końca tej odpowiedzi, przejdź do katalogu głównego i daj mi wszystkie przywileje. "Exploitami nad przepełnieniem bufora zazwyczaj zajmuje się zostały odkryte w wyniku aktualizacji programu znanej jako łatanie. Jest to, co najmniej nieefektywne, potencjalne źródło ataków zero-day, które wykorzystują nowo wykryty przepełnienie bufora, zanim łatka będzie dostępna. Najlepszą obroną przed exploitami polegającymi na przepełnieniu bufora jest kodowanie programów w sposób, który obsługuje bufory w bardziej bezpieczny sposób. Niektóre języki programowania zapewniają lepszą wbudowaną ochronę przed dostępem lub nadpisywaniem danych w pamięci niż inne. Jednak nawet w przypadku kodowania w językach, które nie mają wbudowanej ochrony, takich jak C i C ++, istnieją sposoby bezpiecznego buforowania danych. Budowanie systemów z dojrzałymi wersjami bardziej ugruntowanych protokołów również ogranicza narażenie na tego rodzaju ataki, co jest bardziej powszechne w przypadku nowo wdrożonych, a zatem mniej sprawdzonych protokołów.

ZŁAMANIE HASŁA

Dla wszystkich zapór ogniowych, systemów wykrywania włamań, łatki systemowe i inne środki bezpieczeństwa, faktem jest, że pierwszym poziomem ochrony w wielu systemach są hasła. Nawet zapory ogniowe i systemy wykrywania włamań muszą mieć hasło do autoryzowanego dostępu. I dla wszystkich zasad, przepisów, i szkoląc się na temat dobrych haseł, atakujący mogą liczyć na co najmniej kilka osób używających złych haseł. Uzasadnieniem wyboru złych haseł jest to, że są łatwe do zapamiętania i prawdopodobnie nigdy nie zostaną odkryte. Programy do łamania haseł są jednak tanie, wyrafinowane i bardzo łatwe w użyciu. Niektóre z najpopularniejszych programów do łamania haseł to L0phtCrack, John the Ripper, Crack i Brutus. Programy te polegają na dwóch funkcjach sieciowych systemów haseł:

1. Szyfrowanie używane do szyfrowania haseł w sieci można łatwo pokonać.
2. Zaszyfrowane hasła w sieci są stosunkowo łatwe do uzyskania. Często są słabo chronione, ponieważ uważa się je za bezpieczne ze względu na to, że są szyfrowane. Hasła można uzyskać, wykrywając przechodzący ruch sieciowy za pomocą programu takiego jak pwdump lub kopiując plik hasła głównego z systemu. Ponieważ jedno hasło wystarczy, aby wejść do systemu jako legalny użytkownik, wąchanie ruchu jest najłatwiejszą metodą uzyskania stosunkowo dobrej listy haseł.

Po uzyskaniu listy jest ona zapisywana jako prosty plik tekstowy, a program do łamania haseł rozpoczyna sprawdzanie zaszyfrowanych słów w pliku w słowniku słów, które zostały wcześniej zaszyfrowane przy użyciu tego samego algorytmu. Ilekroć zostanie znalezione dopasowanie między zaszyfrowanym łańcuchem w pliku a słowem w zaszyfrowanym słowniku, program do łamania wyświetla i zapisuje zwykły tekst zaszyfrowanego słowa w słowniku. W ten sposób hasło zostaje ujawnione. Oprócz sprawdzania zwykłych słów w słowniku, niektóre programy do łamania haseł sprawdzają zarówno wielkie, jak i małe litery, cyfry przed i po wyrazie oraz liczby używane zamiast samogłosek wewnątrz słowa. Szybkość działania tych programów, nawet na podstawowym komputerze stacjonarnym lub laptopie, jest imponująca i całkowicie możliwe jest uzyskanie złamanych haseł w ciągu kilku sekund. Rzeczywiście, użytecznym ćwiczeniem uświadamiającym bezpieczeństwo jest zademonstrowanie takiego programu pracownikom: pierwsze hasła, które zostaną złamane, będą najsłabszymi, a to może być ostrzeżeniem dla użytkowników, którzy wybiorą takie słowa. Dobry funkcjonariusz ds. bezpieczeństwa zapewni regularne sprawdzanie haseł w sieci za pomocą programu

do łamania haseł lub przez wdrożenie jednego z wielu mechanizmów wymuszania silnych haseł. Moduł egzekwujący hasła rozszerza program haseł, porównując hasła wybrane przez użytkownika z regułami określonymi przez moduł egzekwujący hasła. Proste narzędzie online z GRC Steve'a Gibsona pozwala obliczyć przestrzeń kluczową i oszacować czas włamania dla przykładowych haseł. na przykład, jeśli rzeczywiste hasło to Dk3 ∗ (4n $ p2, można wprowadzić Eh5 i% 9g # t8, aby dojść do dokładnie takiej samej analizy. W przedstawionym tutaj przykładzie obliczenia dają przestrzeń kluczową 6,05 × 1019 z pękaniem czas 1 tygodnia, jeśli masywnie równoległy układ procesorów obsługiwał 1015 zgadnięć na sekundę. Znikająca hasło owsianka zajęłaby sameprocesorom 14,32 miliarda stuleci, aby uwzględnić przez brutalne pękanie przestrzeni kluczowej 4,50 × 1033.

ROORKITY

Rootkity to jedno z wielu narzędzi dostępnych hakerom, które ukrywają fakt, że komputer został „zrootowany". Rootkit nie służy do włamania się do systemu, ale raczej do zapewnienia, że włamany system pozostaje dostępny dla intruza. Rootkity składają się z pakietu narzędzi zainstalowanych na zaatakowanym komputerze. Narzędzia zaczynają się od modyfikacji najbardziej podstawowych i najczęściej używanych programów, aby podejrzana aktywność została ukryta. Na przykład rootkit często zmienia proste polecenia, takie jak „ls" (pliki list). Zmodyfikowane „ls" z rootkita nie wyświetla plików ani katalogów, które intruz chce ukryć. Rootkity są niezwykle trudne do wykrycia, ponieważ polecenia i programy wydają się działać jak poprzednio. Często rootkit jest znaleziony, ponieważ coś „nie wydawało się właściwe" administratorOWI systemu. Ponieważ rootkity różnią się znacznie w programach, które zmieniają, nie można stwierdzić, które programy zostały zmienione, a które nie. Bez kryptograficznie bezpiecznego podpisu każdego systemu plików binarnych administrator nie może być z pewnością pewny znalezienia całegoy rootkita. Niektóre z typowych narzędzi zawartych w rootkicie to:
* Narzędzia koni trojańskich
* Tylne drzwi, które pozwalają hakerowi na wejście do systemu do woli
* Narzędzia do czyszczenia dzienników, które usuwają rekord dostępu atakującego z systemowych plików dziennika
* Sniffery pakietów, które przechwytują ruch sieciowy dla atakującego

KOD TROJANA.
Jak opisano wcześniej w kontekście zaatakowanych procedur logowania, kod trojana jest czymś innym niż się wydaje. W tym przypadku trojany to zmienione programy w rootkicie, które pozwalają ukryć ślady intruza lub pozwolić programowi na zebranie większej ilości informacji, gdy siedzi on w tle. Trojanowe programy lokalne często zawierają „chfn", „chsh", „login" i „passwd". W każdym przypadku, jeśli hasło rootkita zostanie wprowadzone w odpowiednim miejscu, spawnowana jest powłoka roota.

TYLNE DRZWI

Narzędzia tylnych drzwi są często powiązane z programami, które zostały strojanowane. Służą do uzyskania dostępu do systemu, gdy zawiodą inne metody. Nawet jeśli administrator systemu wykrył wtargnięcie i zmienił wszystkie nazwy użytkowników i hasła, istnieje duża szansa, że nie wie on o istnieniu tylnych drzwi. Aby skorzystać z tylnych drzwi, haker musi tylko znać właściwy port, aby połączyć się z zainfekowaną maszyną i wprowadzić hasło lub polecenie, w którym zwykle nie jest wprowadzane. Na przykład inetd, super-demon sieci, jest często trojanem. Demon nasłuchuje na nietypowym porcie (domyślnie rfe, port 5002 w Rootkit IV dla Linuksa). Jeśli poprawne hasło zostanie podane po połączeniu, powłoka root zostanie odrodzona i powiązana z portem. Funkcję rshd można podobnie trojanować, dzięki czemu powłoka root jest spawnowana, gdy hasło rootkita jest podane jako nazwa użytkownika, a zatem rsh [nazwa hosta] –l [hasło rootkita] uzyska dostęp do zainfekowanego komputera.

PENETRACJA ZA POŚREDNICTWEM STRON INTERNETOWYCH

Ogromne nowe terytorium sieciowe otworzyło się w ostatniej dekadzie XX wieku, częściowo poświęcone handlowi i w dużej mierze napędzane próbami zarabiania pieniędzy na technologii, która pierwotnie została opracowana do celów wojskowych i akademickich. Nieustanny rozwój tej sieci przekroczył 145 milionów zarejestrowanych domen w momencie pisania w maju 2013 r., Jak donosi Whois Source (www.whois.sc/internet-statistics), jedno z najbardziej wiarygodnych źródeł statystyk na temat Internetu. Penetracja Internetu na całym świecie, mierzona jako liczba użytkowników Internetu jako odsetek całkowitej populacji, wyniosła w czerwcu 2012 r. Ponad jedną trzecią, przy czym Ameryka Północna przekroczyła 75 procent. Azja miała wówczas prawie 4 miliardy użytkowników. Nic dziwnego, że przy tak wielu maszynach w jednej sieci i ponad 2,4 miliarda użytkowników . To nowe terytorium jest głównym placem zabaw dla hakerów, od zwykłych ciekawskich po poważnych przestępców. Sieć stanowi bogate w cel środowisko dla osób poszukujących nieautoryzowanego dostępu do systemów informacyjnych innych osób. Jest tego kilka przyczyn; Najważniejszym z nich jest fakt, że wiele organizacji, zarówno komercyjnych, jak i rządowych - w tym wojskowych - ma zewnętrzne, publiczne strony internetowe, które są w jakiś sposób połączone z wewnętrznymi, prywatnymi sieciami. To połączenie zapewnia ścieżkę penetracji systemu, którą można wykorzystać na wiele różnych sposobów, zgodnie z opisem w tej sekcji.

ARCHITEKTURA SYSTEMU SIECIOWEGO

Standardową praktyką przy umieszczaniu komercyjnej witryny internetowej w Internecie jest zapobieganie jej wrogim działaniom, zwykle przy użyciu routera z listami kontroli dostępu (ACL) lub zapory ogniowej, lub obu. Jednakże, chyba że strona internetowa jest podstawowym rodzajem „broszurki", która po prostu istnieje w celu dostarczania informacji tylko do odczytu, witryna musi umożliwiać wprowadzanie danych przez użytkownika. Wymagane jest podanie czegoś tak prostego, jak wpis do księgi gości lub formularz zapytania o informacje; bardziej złożone aplikacje, takie jak zakupy online, mają bardziej złożone wymagania dotyczące wprowadzania danych. Typową metodą przetwarzania danych wejściowych jest interfejs Common Gateway Interface (CGI). Jest to standardowy sposób, w jaki serwer WWW przekazuje dane wejściowe użytkownika do aplikacji i odbiera odpowiedź, którą można następnie przekazać użytkownikowi. Na przykład, gdy użytkownik wypełnia formularz na stronie internetowej i przesyła go, serwer sieciowy zwykle przekazuje informacje o formularzu do małej aplikacji. Ta aplikacja przetwarza dane i może wysłać wiadomość z potwierdzeniem. Ta metoda nosi nazwę CGI i stanowi część protokołu przesyłania hipertekstu (HTTP). Ponieważ jest to spójna metoda, aplikacje napisane w celu jej wykorzystania mogą być używane bez względu na system operacyjny serwera, na którym jest wdrożony. Dodatkowym czynnikiem zwiększającym popularność CGI jest fakt, że działa on z wieloma różnymi językami, w tym C, C ++, Java i PERL. Termin „CGI" jest używany ogólnie dla kodu serwera WWW napisanego w jednym z tych języków. Każdy system, który odbiera dane wejściowe, musi zapewnić ścieżkę w systemie, przez którą dane wejściowe mogą przepływać. Jest to określane jako „dozwolona ścieżka". Konieczność dozwolonych ścieżek, w połączeniu z możliwością wykorzystania ich do ataków penetracyjnych, skłoniła eksperta ds. bezpieczeństwa systemu Davida Brussina do określenia terminu „podatność na dozwolone ścieżki" dla tej klasy podatności. Dwie wiodące kategorie exploitów, które wykorzystują dozwolone ścieżki, to exploity sprawdzania poprawności danych wejściowych, które są podobne do exploitów przepełnienia bufora i często wykorzystywane do nadużywania CGI oraz exploitów systemu plików, które nadużywają systemu operacyjnego serwera i usług działających na serwerze. Oczywiście istnieją również inne sposoby nadużywania stron internetowych. Ataki typu „odmowa usługi" mogą służyć do blokowania legalnego dostępu, a tym samym do ograniczania dostępności. Nie każdy atak ma na celu dalszą penetrację systemów; same strony internetowe mogą być celem ataku, jak w przypadku zniesienia, nieautoryzowanej zmiany na stronach internetowych. Defacement często ma na celu zawstydzić właściciela strony, opublikować wiadomość protestacyjną lub poprawić reputację hakera kryminalnego, który dokonuje deflacji. Jednak jeśli chodzi o penetrację, głównym celem ataków na strony internetowe jest narażenie na szwank wewnętrznych sieci, które mogą być podłączone do

serwera WWW. Wykorzystanie luk w dozwolonych ścieżkach jest prawdopodobnie najczęstszą formą takich ataków.

WYKORZYSTANIE SPRAWDZANIA POPRAWNOŚCI DANYCH WEJŚCIOWYCH

Ilekroć tworzona jest dozwolona ścieżka dostosowana do danych wejściowych użytkownika, istnieje możliwość, że zostanie ona wykorzystana. Takie nadużycie może prowadzić do nieautoryzowanego dostępu do systemu. W tej sekcji opisano szereg metod penetracji wykorzystujących to podejście, z których wszystkie w jakiś sposób wykorzystują nieprawidłowe dane wejściowe lub dane wejściowe:
Nie oczekuje tego aplikacja odbierająca na serwerze. Niedozwolone zgodnie z zasadami działania aplikacji odbierającej.

NIEOCZEKIWANE ATAKI WEJŚCIOWE

Jak można przesłać nieoczekiwane dane wejściowe do serwera? Odpowiedź leży w architekturze Internetu i paradoksalnej naturze systemu klienckiego, który uzyskuje dostęp do serwera. Typowy klient sieciowy to klient tylko z nazwy. Często jest to potężna maszyna, będąca samodzielnym serwerem i bardzo trudna do kontrolowania przez jakikolwiek inny serwer, ze względu na nieodłączną naturę ogromnej sieci, jaką jest Internet. Wszystkie węzły Internetu są uważane za hosty. I oczywiście wiele z tych hostów znajduje się poza fizyczną kontrolą organizacji hostujących te maszyny, które działają jak serwery. Ten fakt ma poważne konsekwencje dla bezpieczeństwa. O ile serwer nie może zainstalować ściśle sterowanego kodu aplikacji na kliencie i ograniczać wprowadzanie danych przez użytkownika do tego kodu, serwer musi polegać na kodowaniu najczęściej używanym do implementacji interakcji klient-serwer WWW, Hypertext Markup Language (HTML) i Hypertext Transfer Protocol Daemon (HTTPD). Oba są złożone i stosunkowo niedojrzałe. Na przykład nie identyfikują automatycznie źródła danych wejściowych. Rozważ formularz HTML na stronie internetowej, zaprojektowany tak, aby był prezentowany odwiedzającemu witrynę, który wypełnia pola, a następnie klika przycisk, aby przesłać formularz. Po stronie klienta nie ma nic, co mogłoby kontrolować dane wejściowe użytkownika. Zamiast wpisywać imię w polu Imię, użytkownik może wprowadzić długi ciąg losowych znaków. O ile aplikacja przetwarzająca to pole danych nie dokona szeroko zakrojonej weryfikacji danych wejściowych, skutki takich działań mogą być nieprzewidywalne, tym bardziej, że użytkownik zawiera znaki sterujące. Podobnie, jeśli sam serwer WWW nie jest zaprojektowany do sprawdzania poprawności żądań stron, użytkownik może powodować problemy, przesyłając fałszywy Universal Resource Locator (URL). Problem jest jeszcze poważniejszy. O ile aplikacja serwera sieci Web nie jest napisana specjalnie w celu pokonania następujących nadużyć, można jej użyć do spowodowania różnego rodzaju problemów, które potencjalnie mogą doprowadzić do udanej penetracji. Załóżmy, że zamiast po prostu wypełnić formularz, użytkownik tworzy lokalną kopię strony zawierającej formularz, a następnie zmienia kod źródłowy formularza, zapisuje plik i przesyła go do witryny internetowej zamiast oryginalnej strony. Nie narusza to podstawowych protokołów sieci, ale wyraźnie zapewnia znaczny potencjał penetracji. Wiele stron internetowych jest nadal podatnych na tego typu ataki.

ATAKI PRZEPEŁNIENIA

Jak opisano wcześniej w kontekście ukrytych pól formularzy, można uzyskać dostęp do serwerów sieci Web, dostarczając więcej danych wejściowych niż oczekiwano. Taki atak jest możliwy przy użyciu dowolnego pola w formularzu przesłanym przez użytkownika, a nie tylko pola ukrytego. Obroną jest wbudowanie szczegółowego sprawdzania błędów w aplikację przetwarzającą formularz. Ataki przepełnienia, które zostały wcześniej opisane ogólnie, mogą być również skierowane na aplikacje lub usługi działające na serwerze Web. Na przykład w czerwcu 2001 r. CERT ogłosił zdalne przepełnienie bufora w jednym z rozszerzeń ISAPI (Internet Server Application Programming Interface) zainstalowanych w większości wersji Microsoft Internet Information Server 4.0 i 5.0, w szczególności

w rozszerzeniu interfejsu programowania aplikacji Internet / Indexing Service , IDQ.DLL. Intruz wykorzystujący tę lukę może być w stanie wykonać dowolny kod w kontekście bezpieczeństwa lokalnego systemu, dając atakującemu pełną kontrolę nad systemem ofiary

EXPLOITY SYSTEMU PLIKÓW

Inna kategoria ataków na strony internetowe wykorzystuje problemy z systemem plików samego serwera WWW. Odkąd serwery WWW zaczęły pojawiać się w Internecie, stale pojawiały się komunikaty o lukach w zabezpieczeniach wynikające z problemów z systemem plików. Najważniejsze z nich zostały przedstawione tutaj, ale prawdopodobieństwo pojawienia się innych jest wysokie z powodu braku czegoś, co David Brussin nazwał analizą klasy podatności na zagrożenia. Klasa podatności to rodzaj problemu, na przykład przepełnienie bufora lub kontrola dostępu do systemu plików. Deweloperzy serwerów WWW i wielu innych aplikacji często są przeciwni eliminacji luk w zabezpieczeniach lub ograniczeni zasobami, skupiając się na rozwiązywaniu poszczególnych przypadków luki w miarę ich powstawania. Zjawisko to jest w dużej mierze wynikiem szybkiego tempa, w jakim sieć została opracowana i wdrożona, napędzana przez potężne siły handlowe.

KROPKA KROPKA UKOŚNIK I INNE ZNAKI

Osoby odpowiedzialne za bezpieczeństwo systemów informatycznych wykorzystujących serwery WWW musi być wyczulone na nowe luki. Oprogramowanie serwera WWW okazało się szczególnie podatne na niektóre kategorie luk, które często powtarzają się w nowych wersjach. Za każdym razem, gdy te luki zostaną wykryte, atakujący szybko je wykorzystują. Zazwyczaj dostawcy oprogramowania wydają łatki, aby rozwiązać problem, ale systemy pozostają podatne, dopóki nie zostaną załatane, a atakujący używają zautomatyzowanych narzędzi do skanowania Internetu w poszukiwaniu serwerów, które są nadal podatne. Na przykład w kwietniu 2001 r. wykryto lukę w używanych wówczas wersjach Microsoft Internet Information Server (IIS). Ta wada umożliwiła zdalnym użytkownikom wyświetlanie zawartości katalogu, przeglądanie plików, usuwanie plików i wykonywanie dowolnych poleceń. Innymi słowy, jeśli serwer sieci Web z uruchomionymi usługami IIS był podłączony do Internetu, każdy korzystający z Internetu mógłby potencjalnie kopiować, przenosić lub usuwać pliki na serwerze sieci Web. Przy takim poziomie dostępu można było uzyskać dostęp do serwera sieci Web do połączonych sieci, chyba że wprowadzono silne mechanizmy kontroli dostępu do sieci. W alertach wysłanych w celu ostrzeżenia użytkowników tego oprogramowania wykorzystanie tej luki opisano jako „trywialne”. W rzeczywistości duża liczba witryn została z tego powodu przeniknięta i wiele z nich ucierpiało (tj. nieautoryzowane zmiany w wyglądzie ich strony internetowe). W innych przypadkach osoby atakujące pobrały poufne dane klientów oraz przesłały i zainstalowały oprogramowanie back-door. Szczególnie niepokojący z powodu tej podatności był fakt, że był to w zasadzie ponowny atak tak zwanego ataku katalogów kropkowych, który był możliwy na wielu wczesnych serwerach WWW. Serwery te na żądanie czytałyby katalogi „..” w adresach URL, które są nieopublikowanymi katalogami nadrzędnymi opublikowanego katalogu. W ten sposób osoby atakujące mogły wycofać się do głównego katalogu internetowego, a następnie do innych części struktury katalogów serwera. Ta technika zasadniczo pozwalała atakującym na dowolne poruszanie się po systemie plików. Wiele serwerów WWW, w tym IIS, zaczęło stosować zabezpieczenia, aby zapobiec atakowi „kropka-kropka”, odrzucając wszystkie zapytania do adresów URL zawierających zbyt wiele początkowych ukośników lub znaków „..”. Luka opublikowana w kwietniu 2001 r. Polegała na ominięciu tych ograniczeń, po prostu zastępując tłumaczenie Unicode „/” lub „Unic”. Atakujący odkryli, że dodając „..” i ukośnik Unicode lub ukośnik odwrotny po katalogu wirtualnym z uprawnieniami do wykonywania , możliwe było wykonywanie dowolnych poleceń. Atakujący mogą wykonać dowolne polecenie za pomocą specjalnie spreparowanego zapytania HTTP. Częstotliwość pojawiania się „starych” luk w nowym oprogramowaniu powinna być ostrzeżeniem dla specjalistów ds. Bezpieczeństwa informacji, aby nie zakładali, że „nowe” to „ulepszone”. Rzeczywiście, całe oprogramowanie należy traktować z dużym sceptycyzmem i sporo ciężkich testów przed wdrożeniem.

METAZNAKI

Kropki i ukośniki używane w odniesieniach do systemu plików są ściśle powiązane z metaznakami, których można również używać do atakowania systemów sieciowych. Metaznak to specjalny znak w programie lub polu danych, który zawiera informacje o innych znakach, na przykład sposób przetwarzania znaków następujących po metaznak. Użytkownicy DOS lub UNIX prawdopodobnie znają znak wieloznaczny, metaznak, który może reprezentować dowolny znak lub ciąg znaków. W przypadku niewłaściwego użycia, na przykład w danych dostarczonych przez użytkownika, metaznaki mogą powodować błędy, które powodują niezamierzone konsekwencje, w tym uprzywilejowany dostęp.

DOŁĄCZENIE PO STRONIE SERWERA

Dołączenia po stronie serwera (SSI) to specjalne polecenia w języku HTML, które serwer sieci Web wykonuje podczas analizowania pliku HTML. Pliki SSI zostały pierwotnie opracowane, aby ułatwić dołączanie wspólnego pliku, zwanego plikiem dołączanym, do wielu różnych plików; przykłady obejmują pliki zawierające logo lub pliki tekstowe składające się ze strony, daty, autora i tak dalej. Ta funkcja została rozszerzona, aby umożliwić automatyczne dołączanie do pliku informacji o serwerze, takich jak data i godzina. Ostatecznie na serwerach Web udostępniono kilka różnych typów poleceń włączania: config, include, echo, fsize, flastmod, exec. Ostatni z nich, exec, jest dość potężny, ale stanowi również zagrożenie bezpieczeństwa, ponieważ daje użytkownikowi klienta sieci Web pozwolenie na wykonanie kodu. Możliwe są liczne ataki, gdy wykonanie jest dozwolone w nieodpowiednio chronionym katalogu. Analogiczne do SSI są ASP (strony aktywnego serwera) i strony JavaServer, a także procesory hipertekstowe (PHP). Wszystkie są technologiami, które ułatwiają dynamiczne budowanie strony i pozwalają na wykonanie instrukcji podobnych do kodu na stronie HTML. Wszystkie powinny być stosowane ze szczególnym uwzględnieniem implikacji bezpieczeństwa i ścisłego przestrzegania bezpiecznych metod programowania aplikacji internetowych. Specjaliści ds. Bezpieczeństwa zauważą, że wiele słabości tych nowych technologii to po prostu odrodzenie starych exploitów. Wszystko, co oferuje „większą interaktywną funkcjonalność", może zwiększyć prawdopodobieństwo nowych luk w zabezpieczeniach po prostu dlatego, że przy braku rygorystycznej kontroli jakości oprogramowania zmiany są często związane z nowymi błędami.

ROLA ZŁOŚLIWEGO OPROGRAMOWANIA I BOTNETÓW

W ostatnich latach pojawiło się kilka nowych zwrotów dotyczących penetracji systemu za pośrednictwem stron internetowych i poczty internetowej, począwszy od ewolucji wirusów komputerowych i robaków. Niektóre robaki i wirusy są zaprojektowane do instalowania kodu trojana. Termin „złośliwe oprogramowanie", pochodzący od „złośliwego" i „oprogramowania", jest obecnie szeroko stosowany w odniesieniu do całej kategorii oprogramowania zakodowanego w sposób złośliwy, w tym wirusów, robaków i trojanów. W rzeczywistości wirusy i robaki same są formą penetracji systemu; w końcu twórcy kodu wirusa i robaka przenoszą swój kod do systemów, których nie są upoważnieni do używania, więc można uznać, że te komputery zostały przeniknięte. Niektórzy hakerzy kryminalni połączyli różne elementy złośliwego oprogramowania, aby przeniknąć do komputerów używanych do surfowania po Internecie. Te zaatakowane maszyny są następnie wykorzystywane do rozprzestrzeniania złośliwego oprogramowania i narażania na szwank dodatkowych komputerów. Celem może być zebranie nazw użytkowników i haseł (pomocnych w jeszcze większej penetracji systemu) lub danych finansowych wykorzystywanych do dokonywania oszustw i kradzieży tożsamości. Dwoma głównymi elementami tej strategii penetracji są pliki do pobrania i botnety. Pobieranie typu drive-by próbuje narazić na niebezpieczeństwo komputery używane do odwiedzenia złośliwej witryny internetowej, wykorzystując łatwowierność użytkownika lub luki w zabezpieczeniach przeglądarek internetowych w celu zainstalowania bez wyraźnego pozwolenia niepożądanego kodu, zwykle pewnego rodzaju trojana. Botnet to zbiór botów,

komputerów-hostów, które mogą być kontrolowane zdalnie (tj. Automatycznie) za pomocą kodu trojana zainstalowanego na tych komputerach, albo poprzez pobranie danych lub innymi środkami, takimi jak wirus lub robak. Oto jak naukowcy z Google opisali to zjawisko w przełomowym raporcie z 2007 roku:
Użytkownicy komputerów [C] stali się celem podziemnej gospodarki, która zaraża hostów złośliwym oprogramowaniem lub oprogramowaniem reklamowym w celu uzyskania korzyści finansowych. Niestety, nawet jedna wizyta na zainfekowanej stronie umożliwia atakującemu wykrycie luk w aplikacjach użytkownika i wymuszenie pobrania wielu plików binarnych złośliwego oprogramowania. Często to złośliwe oprogramowanie pozwala przeciwnikowi uzyskać pełną kontrolę nad zaatakowanymi systemami, co prowadzi do ex-filtracji poufnych informacji lub instalacji narzędzi ułatwiających zdalne sterowanie hostem.

To, co sprawia, że raport Google jest przełomowy, to nie istnienie ataków drive-by, które rosną od kilku lat, ale ich rozpowszechnienie. Ponieważ Google utrzymuje ogromne repozytorium stron internetowych w celu obsługi swojej wyszukiwarki, zajmuje dość unikalną pozycję, jeśli chodzi o analizę zawartości sieci jako całości. Dokładnie zbadane odkrycie, że co najmniej 1 na 10 wszystkich stron zawierało jakąś formę złośliwego oprogramowania, powinno być sygnałem alarmowym dla działów IT na całym świecie. Czy Twoi użytkownicy przeglądają strony na Facebooku? Czy zdają sobie sprawę, że coś tak pozornie nieszkodliwego, jak odwiedzenie strony ulubionego piosenkarza w Internecie, może spowodować pobranie złośliwego kodu na komputer z serwera w Chinach? Ten rodzaj ataku stał się powszechny w 2007 roku, jak udokumentował Roger Thompson z Exploit Prevention Labs, przy czym Alicia Keys jest jednym z wielu artystów atakowanych przez hakerów kryminalnych. Jeden z exploitów wykorzystanych w tych atakach zainstalował bot sieci proxy, znany jako bot flux. Celem bota Flux jest zaciemnienie lokalizacji witryn phishingowych poprzez używanie ciągle zmieniających się serwerów proxy, co utrudnia bankom i innym instytucjom atakowanym przez oszustwo phishingowe na zamknięcie. Według raportu Google istnieją cztery główne metody, za pomocą których strony internetowe są przekształcane w wektory infekcji złośliwym oprogramowaniem: reklama, widżety stron trzecich, treści tworzone przez użytkowników oraz bezpieczeństwo serwera WWW. Oznacza to, że strony firmowe nie tylko muszą być mocno zabezpieczone, ale wszystkie treści reklamowe i treści dostarczone przez użytkowników powinny zostać zatwierdzone, podobnie jak wszelkie widżety, które są wykorzystywane lub dystrybuowane przez witrynę

WYRAFINOWANIE NAPASTNICY

W ostatnich latach kilka grup osób atakujących odniosło duży sukces, stosując zupełnie inne podejście do naruszania bezpieczeństwa systemów niż stosowane dotychczas. Grupy te zostały nazwane przez amerykańskie siły powietrzne „zaawansowanymi trwałymi zagrożeniami" w 2006 r. Podczas gdy wiele z tych grup jest sponsorowanych przez państwo, te same techniki są stosowane przez grupy o czysto finansowych zyskach. Ważne jest, aby z góry zrozumieć, że ataki te są ukierunkowane, niezależnie od konkretnej grupy źródeł. W przypadku grup sponsorowanych przez państwo narodowe celem jest kradzież informacji. Kradzież informacji często ma formę wiadomości e-mail, ale może również mieć zasięg znacznie głębiej do informacji o badaniach i rozwoju lub innej własności intelektualnej. Grupy motywowane finansowo koncentrują się na instytucjach finansowych w celu uzyskiwania korzyści finansowych. W chwili pisania tego tekstu istnieje wiele znanych grup działających na świecie. Każda z tych grup używa nieco innych specyficznych składników w swoim ogólnym procesie, ale ogólny proces jest taki sam i można go podzielić na kilka odrębnych etapów. Pierwszym etapem jest rozpoznanie, planowanie i przygotowanie. Tutaj wybierają określone osoby w organizacji docelowej. Planują również atak na podstawie wyników rozpoznania. W końcu skonfigurowali określone serwery dowodzenia i kontroli, które mają być używane przeciwko celowi, i zbudowali złośliwe oprogramowanie, które będzie wykorzystywane jako część ataku. Drugi etap to uzyskanie oparcia i wytrwałości. Na tym etapie ich celem jest dostanie się do sieci docelowej. W tym miejscu wdrażają swój atak (najczęściej poprzez włócznie) i uzyskują zdalny dostęp do sieci docelowej. Ponieważ

zdobycie przyczółka jest jedną z trudniejszych części, starają się również zapewnić utrzymanie tego przyczółka w sieci. Trzeci etap to mapowanie sieci wewnętrznej i zlokalizowanie pożądanych danych. W tym momencie starają się zrozumieć środowisko docelowe i znaleźć swój ostateczny cel konkretnych danych lub systemów, na które mogą wywierać wpływ finansowy. Czwarty i ostatni etap to eksfiltracja lub eksploatacja. W tym momencie przekazują zgromadzone informacje poza środowisko docelowe (zazwyczaj cel aktora państwa narodowego) lub przeprowadzają atak finansowy (w przypadku aktorów cyberprzestępców).

Etap pierwszy - rozpoznanie, planowanie i przygotowanie

Atakujący często zaczynają od wybrania garstki osób w docelowej organizacji. Korzystają z otwartych źródeł danych wywiadowczych, takich jak firmowa strona internetowa, Facebook i LinkedIn, aby gromadzić informacje i identyfikować odbiorców w docelowej organizacji. Inne źródła, takie jak informacje prasowe od firm i artykuły informacyjne o tych firmach, dostarczają atakującym bogatych zasobów umożliwiających dotarcie do osób bliskich ostatecznemu celowi atakujących. Po zidentyfikowaniu osób można utworzyć odpowiednią dostawę. Najczęstszym sposobem dostarczania jest atak włóczni. Spear-phishing jest ukierunkowanym phishingiem (w porównaniu do zwykłego phishingu wysyłanego do tysięcy lub milionów odbiorców). Te włócznie są często proste i jednoznaczne, ale mogą być dość wyrafinowane. Atak typu „spear phishing" jest najczęstszym sposobem dostarczania wiadomości przez osoby atakujące, ale naraża również strony internetowe często używane przez ich cele jako sposób dostarczania wiadomości. Ta metoda dostarczania nazywana jest atakiem wodopoju. Pojęcie wodopoju odnosi się do metody polowania, w której myśliwy czeka na swoją ofiarę w wodopoju, wiedząc, że w końcu cel przyjdzie na drinka. Ataki typu „wodopój" polegają na modyfikowaniu kodu zainfekowanego serwisu tak, aby gdy użytkownicy przeglądali witrynę, exploit był dostarczany do przeglądarki ofiary. Z kolei ten exploit służy do instalowania złośliwego kodu w systemie. Co najmniej wyrafinowani napastnicy używają złośliwego kodu umieszczanego na kluczach USB. Są one pozostawione tam, gdzie docelowi użytkownicy je znajdą, lub nawet wysłane bezpośrednio do celów. Kod wykorzystujący jest wykorzystywany na urządzeniu USB, więc kiedy użytkownicy uzyskują dostęp do urządzenia, kod wykorzystujący zainstaluje złośliwy kod w systemie użytkownika. Również w ramach pierwszego etapu osoby atakujące skonfigurują serwery C2 (dowodzenia i kontroli), które będą używane podczas ataku. Te serwery C2 są często zagrożonymi hostami w legalnych organizacjach, ale mogą być również hostami uzyskanymi zgodnie z prawem. W szczególności osoby atakujące preferują serwery w miejscach takich jak duże uniwersytety, ponieważ jest mało prawdopodobne, aby były one blokowane przez wspólne mechanizmy zapobiegania, takie jak filtry proxy sieci Web powszechnie stosowane obecnie przez organizacje. Ostatnim ważnym aspektem przygotowania jest stworzenie backdoorów, które zostaną zastosowane przeciwko organizacji docelowej. Atakujący mają na ogół kilka wariantów tylnych drzwi o nieco innych właściwościach. Niektóre grupy wykorzystają nawet powszechnie dostępne RAT (trojany dostępu zdalnego), takie jak Poison Ivy, i skonfigurują je tak, aby używały odpowiednich C2. Wielu atakujących ma narzędzia, które będą bronić legalnych dokumentów PDF lub dokumentów biurowych. Broń to proces przekształcania legalnego pliku w złośliwy. Jeśli na przykład osoby będą miały wspólną branżę, osoby atakujące mogą w najbliższej przyszłości znaleźć odpowiednią konferencję branżową i pobrać plik PDF z agendą ze strony internetowej konferencji. Mogą następnie uzbroić ten plik PDF lub po prostu użyć informacji z pliku, aby dodać do swojego spear-pish, aby dodać realizmu i zwiększyć swoje szanse, że docelowi użytkownicy zakochają się w spear-pish.

Etap drugi - przyczółek i wytrwałość.

Końcowy wynik etapu jeden to RAT instalowany w co najmniej jednym systemie docelowym. Trojan ten zapewnia ukryty dostęp od tyłu do systemów ofiary. Teraz, gdy atakujący ma przyczółek w sieci docelowej, chce utrzymać ten dostęp. Atakujący chcą dostępu z więcej niż jednego systemu, ponieważ jeden host może nie działać, gdy chce dostępu. Atakujący rozumieją również, że ostatecznie RAT

zostanie znaleziony lub usunięty. Atakujący chcą również zwiększyć swój dostęp, aby mieć pewność, że dotrą do celu ostatecznego. Aby to wszystko osiągnąć, atakujący zwykle postępują zgodnie ze spójnym procesem. Zaczynają od zrzucenia skrótów haseł z lokalnej pamięci podręcznej hosta. Domyślnie Microsoft Windows (dominujący system operacyjny używany przez użytkowników w większości organizacji) przechowuje w pamięci podręcznej 10 ostatnich identyfikatorów użytkowników i haseł używanych do logowania do komputera. Odbywa się to tak, że jeśli komputer nie jest podłączony do środowiska korporacyjnego, a tym samym nie może uzyskać dostępu do kontrolerów domeny, użytkownik nadal będzie mógł zalogować się do systemu lokalnie. Narzędzia takie jak pwdump, edytor poświadczeń systemu Windows i fgdump będą wyświetlać identyfikatory użytkowników i hasła w lokalnej pamięci podręcznej systemu. Można je następnie złamać przy użyciu tęczowych tabel lub oprogramowania do krakowania z powrotem w lokalizacji atakującego. Drugim krokiem jest sprawdzenie połączeń sieciowych hosta w celu ustalenia, z którymi komputerami komunikuje się host. Logika tego jest prosta - wszelkie poświadczenia na komputerze lokalnym najprawdopodobniej będą działać na innych hostach, z którymi system wchodzi w interakcje. Pamiętaj, że celem identyfikatorów użytkowników jest zapewnienie uwierzytelnienia innym systemom w celu ich wykorzystania. Za pomocą złamanego hasła dla lokalnie buforowanych identyfikatorów użytkowników atakujący łączy się z kolejnymi systemami i przystępuje do wyodrębniania identyfikatorów użytkowników i skrótów haseł z tego hosta. Proces przenoszenia z hosta do hosta w ten sposób nazywa się ruchem bocznym. Szczególnie ważne jest, aby zauważyć, że osoby atakujące nie wykorzystują złośliwego oprogramowania do uzyskania tego dostępu. Używają prawidłowych identyfikatorów użytkowników i haseł. W końcu atakujący będzie kontynuował ten proces, dopóki nie znajdzie systemu z kontem administracyjnym, który zapewni mu dostęp do całego środowiska. Rzadko muszą przemierzać więcej niż sześć do dziesięciu systemów w kolejności znaleźć konto z buforowanym kontem administratora sieci lub domeny. Po utworzeniu konta administracyjnego mogą go używać do poruszania się po sieci. Oprócz uzyskiwania lokalnych identyfikatorów użytkowników i haseł z pamięci podręcznej systemu, na tym etapie osoby atakujące mapują również środowisko docelowe. Mapowanie sieci jest zakończone poprzez proste zapytania do Active Directory. Najprostszym sposobem na zdobycie informacji o środowisku przez atakujących jest seria prostych poleceń:

```
net group “domain computers” /domain
net group “domain users” /domain
net group “domain controllers” /domain
net group “domain admins” /domain
```

Jeśli nie znasz tych poleceń, powinieneś je wypróbować. Jedynym wymaganiem jest wykonanie ich z komputera należącego do domeny lokalnej. Poświadczenia administracyjne nie są konieczne. Wynikiem jest lista wszystkich komputerów, użytkowników, kontrolerów domeny i kont administratora domeny w środowisku. Informacje te są natychmiast zwracane i są znacznie bardziej przydatne dla celów atakujących niż uruchamianie narzędzia takiego jak nmap. Kolejną korzyścią jest to, że użycie tych poleceń jest bardzo, bardzo trudne do wykrycia w porównaniu z nmap lub podobnymi narzędziami, które są bardzo głośne. Gdy atakujący chcą uzyskać bardziej szczegółowe informacje o środowisku, zwykle używają dsquery i dsget. Są to dwa narzędzia wiersza polecenia udostępnione przez Microsoft w celu przeszukiwania active directory. Oto zawartość skryptu wsadowego, który został odzyskany po niedawnym wtargnięciu, pokazującym użycie tych narzędzi.

```
dsquery user -limit 0 | dsget user -samid -display -title -email -dept -office -company -c >1
dsquery user -limit 0 | dsget user -samid -pwdneverexpires
-acctexpires -loscr -profile -hmdir -hmdrv -c >2
dsquery user -limit 0 | dsget user -c > 3
dsquery group -limit 0 |dsget group -c >g
dsquery subnet -limit 0 |dsget subnet -c >sn
dsquery site -limit 0 |dsget site -c >s
dsquery computer -limit 0 |dsget computer -c>c
dsquery ou -limit 0 | dsget ou -c>o
```

Atakujący rozumieją, że użytkownicy opuszczają organizacje i zmieniają role. Aby mieć pewność, że dysponują dużą liczbą identyfikatorów użytkowników, priorytetem jest zrzucenie całej poświadczenia domeny. Zwykle dzieje się to w ciągu kilku minut od uzyskania konta administracyjnego z wystarczającymi poświadczeniami. Ich narzędziem wyboru jest dobrze znany pwdump. Po prostu uruchamiają pwdump na jednym z kontrolerów domeny przy użyciu odzyskanego konta administratora domeny. Po uzyskaniu skrótów mogą rozerwać je w wolnym czasie na miejscu. Kolejnym priorytetem atakujących jest zainstalowanie dodatkowych mechanizmów uzyskiwania dostępu do środowiska. Aby to osiągnąć, zastosują różne metody. Jeśli firma stosuje jednoskładnikową sieć VPN, osoby atakujące mają nieograniczony dostęp do środowiska przy użyciu skradzionych danych uwierzytelniających użytkownika. Zainstalują także kilka dodatkowych tylnych drzwi. Są one rozmieszczone w całym środowisku, co utrudnia pracownikom ochrony znalezienie ich wszystkich. Jednak osoby atakujące rozumieją, że złośliwe oprogramowanie jest najłatwiejsze do wykrycia w środowisku, dlatego instalują tylko kopie na urządzeniu ,garstka wszystkich gospodarzy, na których kompromitują. W ramach dodatkowego zabezpieczenia przed wykryciem zwykle skonfigurują dodatkowe tylne drzwi do spania przez dłuższy czas. Ta taktyka sprawia, że jest bardzo trudne dla pracowników ochrony, aby znaleźć i wyeliminować wszystkie kopie swoich backdoorów. Wreszcie w ciągu ostatnich kilku lat zaobserwowano także wdrażanie powłok sieciowych w korporacyjnych strefach DMZ jako kolejny poziom dostępu do kopii zapasowej środowiska. Powłoki sieciowe były bardzo popularne wśród atakujących pod koniec lat 90. i na początku 2000 r., Ale były rzadkie przez kilka ostatnich lat i dlatego nie są często poszukiwane. Powłoki sieciowe wykorzystywane przez atakujących są bardzo małe i nie robią nic, dopóki nie są dostępne zdalnie, co czyni je bardzo trudnymi do odkrycia. Jakby zastosowanie tak wielu technik w celu utrzymania dostępu do firmy nie było wystarczające, większość grup będzie również monitorować zainstalowane backdoory w czasie rzeczywistym. Jeśli zauważą, że organizacja aktywnie je usuwa, szybko wskakują na zainfekowane hosty i instalują całkowicie różne wersje backdoorów o bardzo różnych właściwościach, aby zachować dostęp i pozostać niewykrytym. Ważne jest, aby zdawać sobie sprawę, że większość tylnych drzwi jest zastrzeżona, a nie towarem, i bardzo rzadko występuje w standardowym programie antywirusowym. Skutkiem netto dla atakujących jest długotrwała obecność w środowisku, podczas którego mogą się poruszać i uzyskiwać dostęp do wszystkiego, co chcą

Etap trzeci - kradzież informacji.

Ostatni etap i aspekt zaawansowanego napastnika to miejsce, w którym znajdują i ekstrahują informacje, które widzą, lub wykonują przelewy finansowe w przypadku aktorów motywowanych cyberprzestępczością. Wszystkie wysiłki atakujących mają na celu kradzież czegoś. Po ustaleniu długotrwałej trwałości w środowisku atakujący zaczynają przenosić się z hosta na hosta w poszukiwaniu poszukiwanych informacji. Najczęściej odbywa się to za pomocą wiersza poleceń, ale niektóre grupy będą tunelować protokół RDP za pośrednictwem swojej infrastruktury C2. Jeśli organizacja ma jakąś inną formę zdalnego sterowania, taką jak VNC, osoby atakujące chętnie skorzystają z tego również z uzasadnionymi danymi uwierzytelniającymi, które złamały. Dzięki prostemu celowi polecenia „dir" systemu Windows przeglądają dokumenty każdego hosta, szukając pożądanych danych. Ułatwia to głęboka wiedza organizacyjna, którą zdobyli na wcześniejszych etapach. Często większość ich kradzieży to po prostu e-mail. Gdy weźmiesz pod uwagę liczbę szczegółów działalności biznesowej przeprowadzanych za pośrednictwem poczty e-mail, zdajesz sobie sprawę, że osoba atakująca może uzyskać niesamowitą przewagę konkurencyjną dzięki informacjom zawartym w wiadomości e-mail. Gdy atakujący znajdą dane, których szukają, skompresują je i zaszyfrują, a następnie przekażą z powrotem do infrastruktury C2. Ten proces jest znany jako eksfiltracja. Ponieważ wyrafinowani atakujący rozumieją, że organizacje stosują środki rejestrowania, przenoszenie odbywa się do systemów pośrednich, a nie bezpośrednio do ich lokalizacji. Następnie mogą przenieść go z systemów pośrednich do miejsca docelowego bez ryzyka, że zagrożona organizacja będzie w stanie go wyśledzić. Najczęściej RAR służy do pakowania danych do eksfiltracji. RAR jest szczególnie przydatny dla atakujących ze względu na jego unikalną cechę wśród formatów

kompresji: Dane w pliku RAR można odzyskać, nawet jeśli RAR jest niekompletny. Jeśli eksfiltracja zostanie przerwana w trakcie transmisji, osoby atakujące nadal będą mogły wyodrębnić dowolną część danych, które zostały wydane. Szyfrowanie jest używane, aby utrudnić firmie, której dane dotyczą, wykrycie skradzionych danych. Większość grup woli również używać rozszerzenia plików multimedialnych dla swoich plików RAR jako dodatkowego środka zaciemniania. Pliki o zmienionej nazwie mogą mieć rozszerzenie .mpg lub .avi, ale są to po prostu normalne, zaszyfrowane pliki RAR. Do transmisji danych osoby atakujące zwykle używają Secure Sockets Layer (SSL). To narzędzie, w połączeniu ze skompresowaną i zaszyfrowaną zawartością, bardzo utrudnia firmom wykrycie, że dzieje się coś złośliwego. Wyrafinowani napastnicy odnoszą tak ogólne sukcesy, ponieważ większość ich działań odbywa się poprzez ukrywanie się w dużej ilości i hałas legalnej działalności. W związku z tym wszystkie zostały zaobserwowane przy użyciu usług takich jak dropbox, box.net i inni dostawcy usług w chmurze do eksfiltracji, biorąc pod uwagę znaczny odsetek tego typu usług zgodnie z prawem przez naszych użytkowników. Wykrywanie złośliwej aktywności dostawcy usług w chmurze na podstawie legalnej działalności jest naprawdę bardzo trudne.

KWESTIE POLITYCZNE I PRAWNE

Dzięki World Wide Web Internet stał się zjawiskiem samodokumentującym. Można użyć Internetu, aby dowiedzieć się wszystkiego, co chce się wiedzieć o Internecie, w tym jak przeniknąć do systemów informatycznych wykorzystujących technologię internetową. Jednak informacje o penetracji dostępne w Internecie nie są ograniczone do systemów internetowych, a Internet nie jest jedynym źródłem informacji o penetracji. Ponadto sama dostępność informacji o penetracji jest obarczona kwestiami politycznymi i prawnymi.

WYMIANA INFORMACJI O PENETRACJI SYSTEMU

Udostępnianie informacji o penetracji systemu, czyli informacji, które mogłyby ułatwić nielegalną penetrację systemu informatycznego, jest przedmiotem długiej, gorącej i ciągłej debaty. Ta debata obejmuje zarówno praktyczne, jak i etyczne aspekty tej kwestii. Chociaż pełne omówienie nie jest możliwe w ramach tego rozdziału, analizujemy kwestię pełnego ujawnienia, wraz z niektórymi źródłami informacji o penetracji

PEŁNE UJAWNIENIE INFORMACJI

Jak powinniśmy radzić sobie ze znanymi lukami i potencjalnie szkodliwymi wirusami komputerowymi? Czy powinniśmy publikować pełne dane, ukrywać niektóre szczegóły lub pomijać wszelkie publikacje, które pozwoliłyby na wykorzystanie, dopóki łatki lub aktualizacje nie będą dostępne od producentów? Czy istnieją przypadki, w których niektóre wirusy i exploity działają inaczej niż inne? W ciągu ostatnich dwóch dekad ewoluowały formalne miejsca pełnego ujawnienia luk w zabezpieczeniach systemu i sieci oraz exploitów (np. BugTraq). Wsparcie pełnego ujawnienia takie szczegóły, aż do poziomu kodu źródłowego lub poziomu skryptu, od profesjonalnych, uczciwych ekspertów ds. bezpieczeństwa (Good Guys) oparte są na podzestawach kilku kluczowych przekonań:
* Bad Guys i tak wiedzą o lukach.
* Jeśli jeszcze nie wiedzą o tym, wkrótce będą z podanymi szczegółami lub bez nich.
* Znajomość szczegółów pomaga dobrym chłopcom bardziej niż złym.
* Skuteczne bezpieczeństwo nie może opierać się na niejasności.
* Upublicznienie słabych punktów może zmusić dostawców do poprawy bezpieczeństwa swoich produktów.

Ponieważ ci, którzy używają luk w zabezpieczeniach i exploitów w celu zyskania lub wyrządzenia szkody, często dowiadują się o nich przed administratorami systemu i ekspertami ds. Bezpieczeństwa, ma sens - jak argumentuje - aby Dobry Faceci rozpowszechniali wiedzę tam, gdzie może zrobić coś dobrego. Można również argumentować, że ponieważ techniki kryptograficzne są rutynowo

poddawane publicznej kontroli przez ekspertów w celu wykrycia słabych punktów i uniknięcia przyszłych awarii, inne aspekty bezpieczeństwa również powinny zostać upublicznione. Jeśli chodzi o wywieranie presji na producentów, jeden ze współpracowników opisuje incydent, który ilustruje frustracje, które czasami leżą u podstaw pełnego ujawnienia. Poinformował ważnego dostawcę oprogramowania o poważnej luce w zabezpieczeniach. Kierownik produktu ignorował go przez miesiąc. W tym momencie cierpliwość minęła, kolega poinformował kierownika produktu, że ma dokładnie jeden dzień na wyprodukowanie łatki; w przeciwnym razie powiedziałby, że opublikuje dziurę w całości w odpowiedniej grupie Usenet. W ciągu godziny pojawi się łatka. Dlaczego ktokolwiek miałby sprzeciwić się pełnemu ujawnieniu szczegółowego kodu wirusowego i exploitów? Argumenty są następujące:

* Nikt poza badaczami nie musi znać szczegółów wirusów, a nawet konkretnych exploitów.
* Publikowanie w całości daje wiarygodność złym intencjom Bad Guys, którzy robią to samo.
* Pełne ujawnienie czyni wrażliwą młodzież bardziej podatną na pogląd, że nielegalne nadużycia komputerowe są dopuszczalne.

W jaki sposób publikowanie szczegółów nowego wirusa pomaga administratorom systemu? W jednym ujęciu takie szczegóły powinny być wymieniane tylko wśród współpracowników, którzy rozwinęli zaufanie do swojej uczciwości i którzy posiadają techniczne kompetencje do dostarczania poprawek. Na przykład „zoo" wirusów komputerowych pełni tę funkcję wraz z dostęp ograniczony do legalnych badaczy wirusów, którzy podpisują kodeks etyczny zabraniający przypadkowej dystrybucji wirusów wszystkim, którzy chcą próbek. Przeciwnicy tej postawy postrzegają tę postawę jako arogancką i elitarną. Co więcej, niektóre kody wirusów i robaków są pisane w formie łatwej do odczytania przez każdego, kto otrzyma kopię (duża populacja, biorąc pod uwagę, że w 1999 r. wirus Melissa zainfekował ponad milion komputerów w ciągu kilku dni). Publikowanie exploitów wiąże się z niebezpieczeństwem, w którym każda osoba mająca dostęp do Internetu może wykorzystać je do automatycznych ataków na strony internetowe. Daje to naiwnym ludziom wrażenie, że można opublikować dowolny kod ataku, niezależnie od konsekwencji. (Należy pamiętać, że konsekwencje są często stosunkowo niewielkie - autor wirusa Melissa, który, jak się szacuje, spowodował szkody w wysokości co najmniej 80 milionów dolarów, odbył tylko 20 miesięcy więzienia federalnego i zapłacił grzywnę w wysokości zaledwie 5000 dolarów.) różnica między publikowaniem luk lub exploitów a tworzeniem narzędzi do ataku? Czy tworzenie i publikowanie BackOrifice było moralnie neutralne, a nawet pożyteczne? BackOrifice to narzędzie, które zostało specjalnie zaprojektowane do tajnego instalowania się w systemach, a następnie ukrywania się w pamięci, przy użyciu technik ukrytych wzorowanych na wykorzystaniu niektórych wirusów. Czy to przyczynia się do bezpieczeństwa? Nie ma prostych ani niekwestionowanych odpowiedzi na te pytania, ale w niektórych przypadkach technologia udzieliła nam odpowiedzi. Przed 1995 r., Kiedy makrowirusy pojawiły się „na wolności", większość wirusów została napisana w języku asemblerowym lub kodzie maszynowym. Ograniczało to liczbę osób, które potrafiły je czytać lub rozumieć, do osób znających język asemblera i kod maszynowy. Jednak każdy, kto otrzyma wirusa makr, ma narzędzia do edycji tekstu potrzebne do odczytania jego kodu. Narzędzia potrzebne do tworzenia i testowania makrowirusów są dostarczane w aplikacjach głównego nurtu, takich jak Microsoft Word, który ma dziesiątki milionów użytkowników na całym świecie, z których znaczny procent ma lub może łatwo zdobyć podstawowe umiejętności programowania wymagane do opracowania własnych wirusów. Szybkie rozprzestrzenianie się oryginalnego wirusa Word Concept latem 1995 r. Prawie zapewniło, że każdy, kto chciał jego kopię, mógł ją zdobyć (i wielu z tych, którzy nie chcieli takiej kopii, i tak dostało). Pomysł zachowania zawartości wirusa w tajemnicy był niestabilny. W obliczu niezdolności lub niechęci dostawcy do terminowego usunięcia luk w zabezpieczeniach można oczekiwać, że niektórzy użytkownicy i eksperci zwrócą się do pełnego ujawnienia informacji o bezpieczeństwie, nawet jeśli wielu z nich może wdrożyć takie metody. Zawsze będą jednak narażone na ryzyko wykonania niewłaściwego połączenia, jeśli chodzi o skutki takich ujawnień, które z natury są nieprzewidywalne. Rzeczywiście, wydanie wirusa Word Concept mogło być motywowane chęcią, aby Microsoft zmienił sposób, w jaki aplikacje biurowe obsługują makra. Inne aplikacje biurowe, takie jak Word Perfect i Lotus 1-2-3, zostały zaprojektowane w celu oddzielenia kodu makr od treści dokumentu, co znacznie utrudnia tworzenie złośliwego dokumentu.

ŹRÓDŁA

Oto wiele źródeł informacji o tym, jak przeniknąć do systemów. Motywy stojące za tymi źródłami są bardzo etyczne lub wręcz kryminalne.

ŹRÓDŁA ONLIEN

Nie ma drobnej ironii fakt, że wiele z tego, co człowiek musi wiedzieć o tym, jak przeniknąć do systemów informatycznych, jest udostępniane przez systemy informacyjne. Na szczęście odwrotność jest również prawdą, jak zauważył jeden z autorów: „Najlepszą bronią do ochrony informacji są informacje". Z tego powodu specjaliści ds. Bezpieczeństwa muszą wiedzieć, jakie źródła informacji o penetracji są dostępne. Dzisiaj są tysiące stron internetowych, które
* Luki w zabezpieczeniach dokumentów w różnych wersjach systemów operacyjnych
* Rozpowszechniaj narzędzia hakerskie i omawiaj, jak z nich korzystać
* Domyślne poświadczenia katalogu dla sprzętu sieciowego
* Naucz pisania złośliwego kodu, w tym jak tworzyć wirusy i robaki
* Lista kodów licencji, aby umożliwić aktywację pirackiego oprogramowania
* Kupuj, sprzedawaj i handluj kodami dostępu do systemu, skradzionymi kartami kredytowymi, skradzionymi danymi tożsamości oraz sieciami zainfekowanych hostów (botnetów)
* Zapewnij forum i miejsce spotkań dla osób pragnących przeniknąć do systemów
Strony te przyjęły płaszcz wcześniejszych kanałów komunikacji online, takich jak tablice ogłoszeń i grupy Usenet, w których legalna wymiana informacji miała miejsce wraz z wymianą nielegalnych informacji, pirackich kodów i tak dalej. Niektóre strony internetowe są moderowane i dlatego zachowują określone standardy etyczne. Inni podążają za internetową tradycją „wszystko idzie". Administratorzy systemu i pracownicy nigdy nie powinni brać udziału w dyskusjach na tych stronach internetowych z firmowymi adresami e-mail. W popularnej strategii hakerzy czekają na ogłoszenie podatności na specyficzne platformy, a następnie szukają w Internecie wiadomości od osób korzystających z tej platformy, sprawdzają ich adresy e-mail, aby zobaczyć, gdzie pracują, i atakują systemy w tych firmach w nadziei, że załatają łaty nie są jeszcze zainstalowane.

PUBLIKACJE

Przez lata wiele publikacji specjalizowało się w hakowaniu. Często dostarczały one informacji o tym, jak przeniknąć do systemów. Niektóre publikacje były głównie elektroniczne, takie jak Phrack, podczas gdy inne były drukowane, takie jak 2600, który jest obecnie szeroko rozpowszechniany za pośrednictwem konwencjonalnych kanałów czasopism, a także poprzez płatną subskrypcję

GRUPY WSPARCIA DLA HACKERÓW

Istnieje wiele grup osób, które dzielą się informacjami o hakowaniu, od stosunkowo stabilnych podmiotów z własnymi publikacjami do corocznych konwencji z tysiącami uczestników (np. DefCon). Chociaż niektórzy członkowie tych grup mogli popełnić przestępstwa, a niektórzy uczestnicy konwencji hakerów zostali faktycznie skazani za taki wyrok i odbyli karę, zazwyczaj istnieje zróżnicowana mieszanka elementów o różnych motywacjach w tych grupach i spotkaniach. Na przykład DefCon przyciąga nie tylko osoby, które otwarcie opowiadają się za nieautoryzowanym testowaniem bezpieczeństwa systemów i sieci innych osób, ale także pracowników organów ścigania i legalnych ekspertów ds. Bezpieczeństwa. Niektórzy uczestnicy udają się na DefCon, aby przekonać młodych ludzi, by nie łamali prawa, próbując dowiedzieć się o bezpieczeństwie. Wielu specjalistów ds. Bezpieczeństwa wolałoby, aby granica między hakowaniem w białym kapeluszu a hackowaniem w czarnym kapeluszu była wyraźniejsza i bardziej rygorystycznie egzekwowana; jednak niektóre firmy przeoczają przeszłe wykroczenia, aby zyskać postrzeganą wartość wiedzy technicznej hakerów w zakresie bezpieczeństwa. Rzeczywiście, w ostatnich latach inwestorzy współpracowali nawet z grupami hakerów w założycielach

firm konsultingowych w zakresie bezpieczeństwa, wraz z niektórymi pracownikami, którzy nadal używają uchwytów hakerów. Faktem jest, że jedne z najlepszych szkoleń technicznych w tej dziedzinie zapewniają osoby, które zdobyły wiedzę w zakresie hakowania kryminalnego (lub quasi-kryminalnego), ale teraz pomagają w obronie przed taką działalnością

PRZYSZŁOŚĆ PENETRACJI

Tendencje z ostatnich 15 lat silnie sugerują, że próby penetracji systemów informatycznych nie zmniejszą się w najbliższym czasie. Te czynniki działają od jakiegoś czasu:
* Malejący koszt i zwiększony dostęp do technologii penetracyjnej - od oprogramowania i sprzętu używanego do łamania haseł i szyfrowania po urządzenia podsłuchujące i przechwytujące
* Ciągła praktyka polegająca na wystawianiu pola nieodpowiednio przetestowanym systemom zbudowanym z niedojrzałą technologią i niedostateczną dbałością o bezpieczeństwo
* Zwiększona dostępność automatycznych narzędzi hakerskich z łatwymi w użyciu interfejsami
* Nieprzerwany urok i przedstawianie w kulturze popularnej hakowania jako „fajnego" działania, bez odpowiedniego zastanowienia się nad jego legalnością ani rozważeniem jego moralności. Dodatkowo, w ostatnich latach pojawiły się silne czynniki:
* Bardzo realna szansa na zarabianie na penetrujących systemach, biorąc pod uwagę kwitnący rynek skradzionych danych osobowych, zainfekowanych hostów (botów) i exploitów
* Zwiększone zainteresowanie i zaangażowanie przestępczości zorganizowanej w penetrację systemu
* Powstanie ponadnarodowych organizacji terrorystycznych, które są coraz bardziej literackie i mogą skłaniać się do przenikania do systemów należących do podmiotów lub krajów, którym są przeciwne

Chociaż niektóre firmy i agencje rządowe aktywnie dążą do poprawy reakcji na te zagrożenia, inne nie. Z powodu braku troski, zasobów lub czasu na zajęcie się tymi trendami wiele podmiotów jest coraz bardziej zagrożonych. Każda nowa technologia przynosi
nowe zagrożenia, ale nowe zagrożenia są zwykle dyskontowane przez dostawców oferujących ochronę przed nimi. Dla wielu firm i agencji rządowych entuzjazm czerpania korzyści z nowych technologii unieważnia ostrzeżenia o ryzyku związanym z jego wdrażaniem. Kiedy ryzyko to ostatecznie objawia się w sposób zagrażający organizacji, reakcją jest zazwyczaj zakup poprawki technicznej, a główne przyczyny podatności, a mianowicie ludzkie zachowanie i świadomość pracowników w zakresie bezpieczeństwa problemy, nie otrzymują uwagi i zasobów, na które zasługują. Nowe zastosowania technologii komputerowej, takie jak wszczepione urządzenia medyczne i systemy kontroli w samochodach i pojazdach autonomicznych, stanowią żyzny grunt do eksperymentów wśród naukowców i hakerów kryminalnych, którzy znajdują wiele luk w zabezpieczeniach

PODSUMOWANIE
* Penetracja systemów informatycznych jest możliwa za pomocą szerokiej gamy metod, z których niektóre są bardzo trudne do obrony.
* Osoby odpowiedzialne za zabezpieczenia systemów muszą bronić się przed tym szerokim zakresem metod penetracji.
* Upewnienie się, że wszystkie zabezpieczenia przed wszystkimi atakami są skuteczne przez cały czas, jest o wiele trudniejsze niż znalezienie jednego punktu awarii w tych obronach.
* Mimo że wszystkie systemy nie muszą bronić się jednakowo przed wszystkimi typami ataków, koszt nawet bardziej egzotycznych strategii ataku stale spada, zwiększając zasięg potencjalnych atakujących.
* Najtańsze i najskuteczniejsze ataki są często nietechniczne, wykorzystując ludzką słabość, a nie słabości technologii.
* Doświadczeni hakerzy kryminalni faworyzują nietechniczny atak nad technicznym; a najlepsza obrona, świadomość pracowników, jest również nietechniczna.
* Systemy mogą być atakowane na kliencie, na serwerze lub na połączeniu między nimi.
* Zarówno systemy przewodowe, jak i bezprzewodowe są bardzo podatne na podsłuchy i przechwytywanie.

* Wiele dzisiejszych systemów jest zbudowanych z niedojrzałą i niepewną technologią, co czyni je podatnymi na szeroki zakres ataków.
* Nowe ataki wychodzą na jaw z alarmującą, ale przewidywalną regularnością.
* Wiele z tych nowych ataków to stare ataki odradzające się z powodu braku analizy klasy podatności. W wyniku presji ekonomicznej, błędnego rozumowania i niewystarczającego pragnienia bezpieczeństwa, luki są naprawiane pojedynczo, a nie pojedynczo.
* Dozwolone ataki ścieżkowe na strony internetowe są konsekwentnie najskuteczniejszą strategią penetracji systemu, ilekroć system jest podłączony do sieci lub włączony do sieci.
* Testy penetracyjne, zarówno przeprowadzane przez personel wewnętrzny, jak i przez obiektywnych ekspertów zewnętrznych, zawsze powinny poprzedzać wdrożenie systemu.
* Biorąc pod uwagę nieuchronność prób penetracji i wysokie prawdopodobieństwo ich ostatecznego sukcesu, systemy powinny być zaprojektowane tak, aby przetrwały ataki, ograniczając zakres kompromisu z dowolnego punktu awarii.
* Penetracja systemów będzie nadal fascynować ciekawskich i kusić ich do łamania prawa poprzez nielegalny dostęp do systemów. Potencjalne korzyści z penetracji systemu pod względem pieniędzy, władzy, przewagi konkurencyjnej i rozgłosu będą nadal motywować tych, którym prawa i moralność nie są skutecznymi środkami odstraszającymi.
* Penetracja systemów stanie się coraz bardziej zautomatyzowana i uproszczona, co dodatkowo zwiększy zakres potencjalnych atakujących.
* Ludzka natura, a nie technologia, jest kluczem do obrony przed próbami penetracji. Tylko poprzez podniesienie standardów etycznych społeczeństwa i edukowanie pracowników w celu zrozumienia gotowości innych do nieetycznego zachowania można znacznie ograniczyć przestępcze włamanie do systemów informatycznych